

# Resources

- [Azure compliance documentation](#)
- [Azure enables a world of compliance ↗](#)
- [Microsoft 365 compliance offerings](#)
- [Compliance on the Microsoft Trust Center ↗](#)
- [What is Azure Government?](#)
- [Explore Azure Government ↗](#)
- [Microsoft for defense and intelligence ↗](#)
- [DoD Cloud Computing Security Requirements Guide ↗](#)
- [FedRAMP documents and templates ↗](#)
- [DoD Instruction 8510.01 ↗ DoD Risk Management Framework \(RMF\) for DoD Information Technology \(IT\)](#)
- [NIST SP 800-37 ↗ Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy](#)
- [NIST SP 800-53 ↗ Security and Privacy Controls for Information Systems and Organizations](#)
- [NIST SP 800-171 ↗ Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations](#)
- [CNSSI 1253 ↗ Security Categorization and Control Selection for National Security Systems](#)
- Controlled unclassified information (CUI) [Registry ↗](#) and CUI [category list ↗](#)

# Azure Policy Samples

Article • 01/04/2024

This page is an index of Azure Policy built-in policy definitions and language use patterns.

## Built-ins

- [Policies](#)
- [Initiatives](#)

## Patterns

The following are examples of different patterns using the language and operators in Azure Policy:

- [Logical operators](#)
- [Fields](#)
- [Parameters](#)
- [Effect details](#)
- [Using tags](#)
- [Value operator](#)
- [Count operator](#)
- [Grouping policy definitions in an initiative](#)
- [Deploying resources with deployIfNotExists](#)

## Regulatory Compliance

The following are the [Regulatory Compliance](#) built-ins in Azure:

- [Australian Government ISM PROTECTED](#)
- [Canada Federal PBMM](#)
- [CIS Microsoft Azure Foundations Benchmark 1.1.0](#)
- [CIS Microsoft Azure Foundations Benchmark 1.3.0](#)
- [CIS Microsoft Azure Foundations Benchmark 1.4.0](#)
- [CIS Microsoft Azure Foundations Benchmark 2.0.0](#)
- [CMMC Level 3](#)
- [FedRAMP High](#)
- [FedRAMP Moderate](#)

- HIPAA HITRUST 9.2
- IRS 1075 September 2016
- ISO 27001:2013
- Microsoft cloud security benchmark
- Microsoft Cloud for Sovereignty Confidential
- Microsoft Cloud for Sovereignty Global
- New Zealand ISM Restricted
- New Zealand ISM Restricted 3.5
- NIST SP 800-53 Rev. 4
- NIST SP 800-53 Rev. 5
- NIST SP 800-171 R2
- NL BIO Cloud Theme
- PCI DSS 3.2.1
- PCI DSS 4.0
- RBI ITF Banks v2016
- RBI ITF NBFC v2017
- RMIT Malaysia
- SWIFT CSP-CSCF v2021
- SWIFT CSP-CSCF v2022
- UK OFFICIAL and UK NHS

The following are the [Regulatory Compliance](#) built-ins in Azure Government:

- CIS Microsoft Azure Foundations Benchmark v1.1.0
- CIS Microsoft Azure Foundations Benchmark v1.3.0
- CMMC Level 3
- FedRAMP High
- FedRAMP Moderate
- IRS 1075 September 2016
- ISO 27001:2013
- Microsoft cloud security benchmark
- NIST SP 800-53 Rev. 4
- NIST SP 800-53 Rev. 5
- NIST SP 800-171 R2

## Other Samples

- [GitHub - Community Policy repo ↗](#)

## Next steps

- See the built-ins on the [Azure Policy GitHub repo](#).
- Review the [Azure Policy definition structure](#).
- Review [Understanding policy effects](#).

# Department of Defense (DoD) Impact Level 5 (IL5)

Article • 04/05/2023

## DoD IL5 overview

The Defense Information Systems Agency (DISA) is an agency of the US Department of Defense (DoD) that is responsible for developing and maintaining the DoD Cloud Computing [Security Requirements Guide \(SRG\)](#). The Cloud Computing SRG defines the baseline security requirements used by DoD to assess the security posture of a cloud service offering (CSO), supporting the decision to grant a DoD provisional authorization (PA) that allows a cloud service provider (CSP) to host DoD missions. It incorporates, supersedes, and rescinds the previously published DoD Cloud Security Model (CSM), and maps to the DoD Risk Management Framework (RMF).

DISA guides DoD agencies and departments in planning and authorizing the use of a CSO. It also evaluates CSOs for compliance with the SRG — an authorization process whereby CSPs can furnish documentation outlining their compliance with DoD standards. It issues DoD provisional authorizations (PAs) when appropriate, so DoD agencies and supporting organizations can use cloud services without having to go through a full approval process on their own, saving time and effort.

According to Section 3.1.3 (Page 19) of the [Cloud Computing SRG](#), IL5 information covers:

- Controlled unclassified information (CUI) that requires higher level of protection than that afforded by IL4
  - The [CUI Registry](#) provides specific categories of information that is under protection by the Executive branch, for example, more than 20 category groupings are included in the [CUI category list](#), such as:
    - Critical infrastructure (for example, Critical Energy Infrastructure Information)
    - Defense (for example, Naval Nuclear Propulsion Information, Unclassified Controlled Nuclear Information – Defense)
    - Export Control (for example, [Export Administration Regulations \(EAR\)](#) restrictions for items on the [Commerce Control List](#), or [International Traffic in Arms Regulations \(ITAR\)](#) restrictions for items on the [US Munitions List](#))
    - Financial (for example, bank secrecy, budget, and so on)
    - Intelligence (for example, Foreign Intelligence Surveillance Act)

- Law enforcement (for example, criminal history records, accident investigations, and so on)
    - Nuclear (for example, [Unclassified Controlled Nuclear Information](#) – Energy)
    - Privacy (for example, military personnel records, health information, and so on)
    - And more
  - The National Institute of Standards and Technology (NIST) [SP 800-171](#) – *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* is intended for use by federal agencies in contracts or other agreements established with non-federal organizations.
- National Security Systems (NSS)
    - [NIST SP 800-59](#) – *Guideline for Identifying an Information System as a National Security System* provides definitions of NSS. As stated on Page 3, NSS means any information system used by an agency which involves:
      - Intelligence activities
      - Cryptologic activities related to national security
      - Command and control of military forces
      - Equipment that is an integral part of weapons systems
      - Functions critical to direct fulfillment of military or intelligence missions

These categories are explained in more detail in Appendix A.1 starting on Page 7. See also Appendix A.2 on Page 9 for examples of questions that an agency may employ to provide clarification of these categories.

- The [Committee on National Security Systems Instruction No. 1253 \(CNSSI 1253\)](#) – *Security Categorization and Control Selection for National Security Systems* provides guidance on the security standards that federal agencies should apply to categorize national security information.

IL5 accommodates NSS and CUI categorizations based on CNSSI 1253 up to moderate confidentiality and moderate integrity (M-M-x). The determination of whether CUI and/or mission data fits the IL5 category is up to the authorizing official responsible for categorizing the information and choosing the cloud impact level.

The [15 December 2014 DoD CIO memo](#) regarding *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services* states that "FedRAMP will serve as the minimum security baseline for all DoD cloud services." The SRG uses the FedRAMP Moderate baseline at all information impact levels (IL) and considers the High Baseline at some.

Section 5.1.1 *DoD use of FedRAMP Security Controls* (Page 37) of the [Cloud Computing SRG](#) states that a FedRAMP High provisional authorization, supplemented with DoD FedRAMP+ controls and control enhancements (C/CEs) and requirements in the Cloud Computing SRG, are used to assess CSOs toward awarding a DoD IL5 PA. No matter what C/CE baseline is used as the basis for a FedRAMP High provisional authorization, extra considerations and/or requirements will need to be assessed and approved before a DoD IL5 PA can be awarded. Moreover, according to Section 5.2.2.3 *Impact Level 5 Location and Separation Requirements* (Page 51), the following requirements (among others) must be in place for an IL5 PA:

- Virtual/logical separation between DoD and federal government tenants/missions is sufficient. Virtual/logical separation between tenant/mission systems is minimally required.
- Physical separation from non-DoD/non-federal government tenants (for example, public, local/state government tenants) is required.

Section 5.6.2 *CSP Personnel Requirements* (Page 76) additionally restricts CSP personnel having access to IL4 and IL5 data to US citizens, US nationals, or US persons. No foreign persons may have such access.

## Azure and DoD IL5

Microsoft maintains the following authorizations for Azure Government regions US Gov Arizona, US Gov Texas, and US Gov Virginia:

- FedRAMP High provisional authorization to operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB)
- DoD IL2 PA
- DoD IL4 PA
- DoD IL5 PA

If you are deploying IL5 workloads in Azure Government regions US Gov Arizona, US Gov Texas, and US Gov Virginia, make sure you review [Isolation guidelines for Impact Level 5 workloads](#) for help with meeting DoD IL5 isolation requirements.

Azure Government has two additional regions, US DoD Central and US DoD East, that are reserved for exclusive use by the US Department of Defense. A separate DoD IL5 PA is in place for Azure Government DoD regions. For more information, see [Department of Defense \(DoD\) in Azure Government](#).

For extra customer assistance, Microsoft provides the Azure Policy regulatory compliance built-in initiative for Azure Government, which maps to DoD IL5 [compliance](#)

**domains and controls:**

- [DoD IL5 Azure Government regulatory compliance built-in initiative](#)

Regulatory compliance in Azure Policy provides built-in initiative definitions to view a list of controls and compliance domains based on responsibility – customer, Microsoft, or shared. For Microsoft-responsible controls, we provide extra audit result details based on third-party attestations and our control implementation details to achieve that compliance. Each DoD IL5 control is associated with one or more Azure Policy definitions. These policies may help you [assess compliance](#) with the control; however, compliance in Azure Policy is only a partial view of your overall compliance status. Azure Policy helps to enforce organizational standards and assess compliance at scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to more granular status.

For more information about Azure support for NIST SP 800-171, see [Azure NIST SP 800-171 documentation](#).

## Applicability

- Azure Government

## Services in scope

For a list of Azure Government cloud services in DoD IL5 PA scope, see [Cloud services in audit scope](#).

Service availability varies across Azure Government regions. For an up-to-date list of service availability, see [Products available by region ↗](#).

## Office 365 and DoD IL5

For more information about Office 365 compliance, see [Office 365 DoD IL5 documentation](#).

## Attestation documents

For access to Azure Government FedRAMP documentation, see [FedRAMP attestation documents](#).

Contact DISA for access to the most recent Azure Government DoD IL5 PA letter.

# Frequently asked questions

What Azure services are covered by DoD IL5 PA and in what regions?

To find out what services are available in Azure Government, see [Products available by region](#). For a list of services provisionally authorized at DoD IL5, see [Cloud services in audit scope](#).

## Resources

- [Azure compliance documentation](#)
- [Azure enables a world of compliance](#)
- [Microsoft 365 compliance offerings](#)
- [Compliance on the Microsoft Trust Center](#)
- [What is Azure Government?](#)
- [Explore Azure Government](#)
- [Microsoft for defense and intelligence](#)
- [DoD Cloud Computing Security Requirements Guide](#)
- [FedRAMP documents and templates](#)
- [DoD Instruction 8510.01](#) *DoD Risk Management Framework (RMF) for DoD Information Technology (IT)*
- [NIST SP 800-37](#) *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- [NIST SP 800-53](#) *Security and Privacy Controls for Information Systems and Organizations*
- [NIST SP 800-59](#) *Guideline for Identifying an Information System as a National Security System*
- [NIST SP 800-171](#) *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*
- [CNSSI 1253](#) *Security Categorization and Control Selection for National Security Systems*
- Controlled unclassified information (CUI) [Registry](#) and CUI [category list](#)
- [Isolation guidelines for Impact Level 5 workloads](#)

# Azure Policy Samples

Article • 01/04/2024

This page is an index of Azure Policy built-in policy definitions and language use patterns.

## Built-ins

- [Policies](#)
- [Initiatives](#)

## Patterns

The following are examples of different patterns using the language and operators in Azure Policy:

- [Logical operators](#)
- [Fields](#)
- [Parameters](#)
- [Effect details](#)
- [Using tags](#)
- [Value operator](#)
- [Count operator](#)
- [Grouping policy definitions in an initiative](#)
- [Deploying resources with deployIfNotExists](#)

## Regulatory Compliance

The following are the [Regulatory Compliance](#) built-ins in Azure:

- [Australian Government ISM PROTECTED](#)
- [Canada Federal PBMM](#)
- [CIS Microsoft Azure Foundations Benchmark 1.1.0](#)
- [CIS Microsoft Azure Foundations Benchmark 1.3.0](#)
- [CIS Microsoft Azure Foundations Benchmark 1.4.0](#)
- [CIS Microsoft Azure Foundations Benchmark 2.0.0](#)
- [CMMC Level 3](#)
- [FedRAMP High](#)
- [FedRAMP Moderate](#)

- HIPAA HITRUST 9.2
- IRS 1075 September 2016
- ISO 27001:2013
- Microsoft cloud security benchmark
- Microsoft Cloud for Sovereignty Confidential
- Microsoft Cloud for Sovereignty Global
- New Zealand ISM Restricted
- New Zealand ISM Restricted 3.5
- NIST SP 800-53 Rev. 4
- NIST SP 800-53 Rev. 5
- NIST SP 800-171 R2
- NL BIO Cloud Theme
- PCI DSS 3.2.1
- PCI DSS 4.0
- RBI ITF Banks v2016
- RBI ITF NBFC v2017
- RMIT Malaysia
- SWIFT CSP-CSCF v2021
- SWIFT CSP-CSCF v2022
- UK OFFICIAL and UK NHS

The following are the [Regulatory Compliance](#) built-ins in Azure Government:

- CIS Microsoft Azure Foundations Benchmark v1.1.0
- CIS Microsoft Azure Foundations Benchmark v1.3.0
- CMMC Level 3
- FedRAMP High
- FedRAMP Moderate
- IRS 1075 September 2016
- ISO 27001:2013
- Microsoft cloud security benchmark
- NIST SP 800-53 Rev. 4
- NIST SP 800-53 Rev. 5
- NIST SP 800-171 R2

## Other Samples

- [GitHub - Community Policy repo ↗](#)

## Next steps

- See the built-ins on the [Azure Policy GitHub repo](#).
- Review the [Azure Policy definition structure](#).
- Review [Understanding policy effects](#).

# Department of Defense (DoD) Impact Level 6 (IL6)

Article • 04/05/2023

## DoD IL6 overview

The Defense Information Systems Agency (DISA) is an agency of the US Department of Defense (DoD) that's responsible for developing and maintaining the DoD Cloud Computing [Security Requirements Guide \(SRG\)](#). The Cloud Computing SRG defines the baseline security requirements used by DoD to assess the security posture of a cloud service offering (CSO), supporting the decision to grant a DoD Provisional Authorization (PA) that allows a cloud service provider (CSP) to host DoD missions. It incorporates, supersedes, and rescinds the previously published DoD Cloud Security Model (CSM), and maps to the DoD Risk Management Framework (RMF).

DISA guides DoD agencies and departments in planning and authorizing the use of a CSO. It also evaluates CSOs for compliance with the SRG — an authorization process whereby CSPs can furnish documentation outlining their compliance with DoD standards. It issues DoD provisional authorizations (PAs) when appropriate, so DoD agencies and supporting organizations can use cloud services without having to go through a full approval process on their own, saving time and effort.

IL6 is reserved for the storage and processing of information classified up to the SECRET level. For a cloud deployment, information that must be processed and stored at IL6 can only be processed in a DoD private/community or Federal government community cloud. Because of the requirement that the entire CSO infrastructure be dedicated and separate from other CSP/CSO infrastructures, IL6 CSOs may only be provided by CSPs under contract to the DoD or a federal agency. IL6 accommodates classified information categorizations up to moderate confidentiality and moderate integrity (M-M-x). Classification does not dictate a high confidentiality and high integrity (H-H-x) information categorization.

The [Committee on National Security Systems Instruction No. 1253](#) (CNSSI 1253), *Security Categorization and Control Selection for National Security Systems*, provides all federal government departments, agencies, bureaus, and offices with a guidance for security categorization of National Security Systems (NSS) that collect, generate, process, store, display, transmit, or receive National Security Information. The National Institute of Standards and Technology (NIST) Special Publication [SP 800-59](#) *Guideline*

*for Identifying an Information System as a National Security System* provides NSS definitions.

CNSSI 1253 builds on the NIST [SP 800-53](#), which provides the FedRAMP control baselines. However, there are some key differences between CNSSI 1253 and NIST SP 800-53, including the approach adopted by CNSSI 1253 to define explicitly the associations of Confidentiality, Integrity, and Availability to security controls, and to refine the use of security control overlays for the national security community. NSS are categorized using separate Low, Medium, and High categorization for each of the security objectives (Confidentiality, Integrity, and Availability). This approach results in categorizations such as "Moderate-Moderate-Low", "Moderate-Moderate-High", and so on. CNSSI 1253 then provides the appropriate security baselines for each of the possible system categorizations using controls from NIST SP 800-53.

The [15 December 2014 DoD CIO memo](#) regarding *Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services* states that "FedRAMP will serve as the minimum security baseline for all DoD cloud services." The Cloud Computing SRG uses the FedRAMP Moderate baseline at all information impact levels (IL) and considers the High baseline at some.

Section 5.1.1 *DoD use of FedRAMP Security Controls* (Page 37) of the [Cloud Computing SRG](#) states that a FedRAMP High provisional authorization, supplemented with DoD FedRAMP+ controls and control enhancements (C/CEs) and requirements in the SRG, are used to assess CSOs toward awarding a DoD IL6 PA. Most IL5 FedRAMP+ C/CEs are also applicable at IL6 in addition to a classified overlay. No matter what C/CE baseline is used as the basis for a FedRAMP High provisional authorization, extra considerations and/or requirements will need to be assessed and approved before a DoD IL6 PA can be awarded. Moreover, according to Section 5.2.2.4 *Impact Level 6 Location and Separation Requirements* (Page 55), the following requirements (among others) must be in place for an IL6 PA:

- IL6 information up to the SECRET level must be stored and processed in a dedicated cloud infrastructure located in facilities approved for the processing of classified information, rated at or above the highest level of classification of the information being stored and/or processed.
- IL6 cloud infrastructure is considered to be a Secret Internet Protocol Router Network (SIPRNet) enclave, and as such will be a closed self-contained environment for the cloud service offering (CSO) processing, storage, and management planes connected only to SIPRNet.
- Virtual/logical separation between DoD and federal government tenants/SECRET missions is sufficient.
- Virtual/logical separation between tenant/mission systems is minimally required.

- Physical separation from non-DoD/non-federal government tenants (for example, public, local/state government tenants) is required.

Section 5.6.2 *CSP Personnel Requirements* (Page 76) imposes extra US citizenship restrictions on CSP personnel with access to IL6 data.

## Azure and DoD IL6

[Azure Government Secret](#) maintains an Impact Level 6 (IL6) DoD provisional authorization (PA) at the high confidentiality, high integrity, and customer-determined availability (H-H-x) information categorization. It provides a direct connection to the DoD Secret Internet Protocol Router Network (SIPRNet) and is operated by cleared US citizens.

### Note

Azure Government Secret is the first and only classified cloud service offering (CSO) to have received the highest possible DoD Impact Level 6 (IL6) provisional authorization (PA) at the **high confidentiality and high integrity (H-H-x)** information categorization.

Developed using the same principles and architecture as Azure Commercial, [Azure Government Secret](#) enables fast access to sensitive, mission-critical information while maintaining the security and integrity of classified workloads. It's available from three accredited regions located over 500 miles apart to support demanding business continuity and disaster recovery requirements. Azure Government Secret operates on secure, native connections to classified networks with options for [ExpressRoute](#) and [ExpressRoute Direct](#) for private, resilient, high-bandwidth connectivity.

## Applicability

- Azure Government Secret

## Services in scope

For a list of Azure Government Secret cloud services in DoD IL6 PA scope, see [Cloud services in audit scope](#). For service availability, contact your Microsoft account representative.

# Attestation documents

Contact DISA for access to the most recent Azure Government Secret DoD IL6 PA letter.

## Frequently asked questions

### What Azure services are covered by DoD IL6 PA and in what regions?

Services that can accommodate IL6 information are available in the Azure Government Secret regions. For a list of services provisionally authorized at DoD IL6, see [Cloud services in audit scope](#). For service availability, contact your Microsoft account representative.

## Resources

- [Azure compliance documentation](#)
- [Azure enables a world of compliance ↗](#)
- [Microsoft 365 compliance offerings](#)
- [Compliance on the Microsoft Trust Center ↗](#)
- [Azure Government Secret ↗](#)
- [Microsoft for defense and intelligence ↗](#)
- [DoD Cloud Computing Security Requirements Guide ↗](#)
- [FedRAMP documents and templates ↗](#)
- [DoD Instruction 8510.01 ↗ DoD Risk Management Framework \(RMF\) for DoD Information Technology \(IT\)](#)
- [NIST SP 800-37 ↗ Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy](#)
- [NIST SP 800-53 ↗ Security and Privacy Controls for Information Systems and Organizations](#)
- [NIST SP 800-59 ↗ Guideline for Identifying an Information System as a National Security System](#)
- [CNSSI 1253 ↗ Security Categorization and Control Selection for National Security Systems](#)

# DoE 10 CFR Part 810

Article • 09/25/2022

## DoE 10 CFR Part 810 overview

The US Department of Energy (DoE) export control regulation [10 CFR Part 810](#) implements section 57b.(2) of the [Atomic Energy Act of 1954](#) (AEA), as amended by section 302 of the [Nuclear Nonproliferation Act of 1978](#) (NNPA). It is administered by the [National Nuclear Security Administration](#) (NNSA). The revised Part 810 (final rule) became effective on 25 March 2015, and, among other things, it controls the export of unclassified nuclear technology and assistance. It enables peaceful nuclear trade by helping to assure that nuclear technologies exported from the United States will be used only for peaceful purposes. Paragraph 810.7 (b) states that specific DoE authorization is required for providing or transferring sensitive nuclear technology to any foreign entity.

## Azure and DoE 10 CFR Part 810

Azure Government can accommodate customers subject to DoE 10 CFR Part 810 export control requirements because it is designed to meet specific controls that restrict access to information and systems to US persons among Azure operations personnel. Azure Government also imposes background screening requirements mandated by US Government on operations personnel with access to production systems. For more information, see [Screening and Azure support for export controls](#).

Aside from controls on operations personnel with access to production systems, Azure Government maintains compliance with rigorous US Government assessments and authorizations, including:

- [FedRAMP High](#) provisional authorization to operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB)
- US Department of Defense (DoD) Cloud Computing Security Requirements Guide (SRG) [Impact Level 5 \(IL5\)](#) provisional authorization (PA) issued by the Defense Information Systems Agency (DISA)

FedRAMP and DoD provisional authorizations are based on the National Institute of Standards and Technology (NIST) [SP 800-53](#) controls. They include provisions for penetration testing and vulnerability scanning, continuous monitoring, Plan of Action & Milestones (POA&M), and so on, to provide assurances that assessed controls are operating effectively.

If you're deploying applications and data to Azure Government, you're responsible for your own security classification process. For data subject to DoE export controls, the classification system is augmented by the [Unclassified Controlled Nuclear Information](#) (UCNI) controls established by Section 148 of the AEA.

## Azure and U-NNPI

The [Naval Nuclear Propulsion Program](#) was created under [Executive Order 12344](#) (see also [50 USC 2511](#)). It comprises the military and civilian personnel who design, build, operate, maintain, and manage the nuclear-powered ships and facilities that support the US nuclear-powered naval fleet. The program provides the design, development, and operational support required for effective military nuclear propulsion plants, and ensures their safe, reliable, and long-lived operation.

Naval Nuclear Propulsion Information (NNPI) that is designated as CUI is listed in the [CUI category list](#). Unclassified NNPI (U-NNPI) is marked Not Releasable to Foreign Nationals (NOFORN), and it may not be released publicly or disclosed to foreign nationals. Table 1 and Exhibit 1 in [OPNAVINST N9210.3](#) *Safeguarding of Naval Nuclear Propulsion Information (NNPI)* discuss the different classification levels/handling controls for NNPI, including access requirements for U-NNPI. Azure Government can accommodate U-NNPI workloads because it is designed to meet specific controls that restrict access to information and systems to US persons among Azure operations personnel. Azure Government also imposes background screening requirements mandated by US Government on operations personnel with access to production systems. For more information, see [Screening](#) and [Azure support for export controls](#). Moreover, an accredited third-party assessment organization (3PAO) has attested that Azure Government has implemented the security controls that are part of the Navy's security overlay. For more information, see [Azure NIST SP 800-171 documentation](#).

### Note

You must contact [Naval Reactors](#) (Naval Nuclear Propulsion Program) to obtain authorization prior to hosting unclassified NNPI (U-NNPI) in Azure Government.

## Applicability

- Azure Government

## Frequently asked questions

## **How does NRC 10 CFR Part 110 relate to DoE 10 CFR Part 810?**

The Nuclear Regulatory Commission [\(NRC\)](#) is responsible for the [Export and import of nuclear equipment and materials](#) under the [10 CFR Part 110](#) export control regulations. The NRC regulates the export and import of nuclear facilities and related equipment and materials. The NRC doesn't regulate nuclear technology and assistance related to these items which are under the DoE jurisdiction. Consequently, the NRC 10 CFR Part 110 regulations wouldn't be applicable to Azure or Azure Government.

## **How can I supply evidence that I am complying with DoE 10 CFR Part 810?**

If your organization is deploying data to Azure Government, you can rely on the Azure Government FedRAMP High P-ATO as evidence that the underlying cloud services platform is handling data in an appropriately restricted manner. However, you're responsible for getting a DoE authorization for your own systems, including the use of cloud services.

## **Can Azure Government accommodate U-NNPI?**

Yes; however, you must contact [Naval Reactors](#) (Naval Nuclear Propulsion Program) to obtain authorization prior to hosting U-NNPI in Azure Government. Naval Nuclear Propulsion Information (NNPI) that is designated as controlled unclassified information (CUI) is listed in the [CUI category list](#). Unclassified NNPI (U-NNPI) is marked Not Releasable to Foreign Nationals (NOFORN), and may not be released publicly or disclosed to foreign nationals. Azure Government can accommodate U-NNPI workloads because it is designed to meet specific controls that restrict access to information and systems to US persons among Azure operations personnel. Azure Government also imposes background screening requirements mandated by US Government on operations personnel with access to production systems. For more information, see [Screening](#) and [Azure support for export controls](#). Moreover, an accredited third-party assessment organization (3PAO) has attested that Azure Government has implemented the security controls that are part of the Navy's security overlay. For more information, see [Azure NIST SP 800-171 documentation](#).

## **What are my responsibilities for classifying data deployed to Azure Government?**

If you're deploying data to Azure Government, you're responsible for your own security classification process. For customer data subject to DoE export controls, the classification system is augmented by the [Unclassified Controlled Nuclear Information](#) (UCNI) controls established by Section 148 of the [Atomic Energy Act of 1954](#) (AEA).

# **Resources**

- [Azure compliance documentation](#)
- [Azure enables a world of compliance](#)

- Microsoft 365 compliance offerings
- Compliance on the Microsoft Trust Center [↗](#)
- What is Azure Government?
- Explore Azure Government [↗](#)
- Microsoft government solutions [↗](#)
- Microsoft for defense and intelligence [↗](#)
- Azure support for export controls
- 10 CFR Part 810 [↗](#)
- Atomic Energy Act of 1954 [↗](#) (AEA)
- Nuclear Nonproliferation Act of 1978 [↗](#) (NNPA)
- National Nuclear Security Administration [↗](#) (NNSA)
- Unclassified Controlled Nuclear Information [↗](#) (UCNI)
- NIST SP 800-53 [↗](#) *Security and Privacy Controls for Information Systems and Organizations*

# Export Administration Regulations (EAR)

Article • 09/25/2022

## EAR overview

The US Department of Commerce is responsible for enforcing the [Export Administration Regulations](#) (EAR) through the [Bureau of Industry and Security](#) (BIS). According to BIS [definitions](#), export is the transfer of protected technology or information to a foreign destination or release of protected technology or information to a foreign person in the United States, also known as deemed export. Items subject to the EAR can be found on the [Commerce Control List](#) (CCL), and each item has a unique [Export Control Classification Number](#) (ECCN) assigned. Items not listed on the CCL are designated as EAR99, and most EAR99 commercial products don't require a license to be exported. However, depending on the destination, end user, or end use of the item, even an EAR99 item may require a BIS export license.

The EAR is applicable to dual-use items that have both commercial and military applications, and to items with purely commercial application. The BIS has provided guidance that cloud service providers (CSP) aren't exporters of customers' data due to the customers' use of cloud services. Moreover, in the [final rule](#) published on 3 June 2016, BIS clarified that EAR licensing requirements wouldn't apply if the transmission and storage of unclassified technical data and software were encrypted end-to-end using FIPS 140 validated cryptographic modules and not intentionally stored in a military-embargoed country (that is, Country Group D:5 as described in [Supplement No. 1 to Part 740](#) of the EAR) or in the Russian Federation. The US Department of Commerce has made it clear that, when data or software is uploaded to the cloud, the customer, not the cloud provider, is the *exporter* who has the responsibility to ensure that transfers, storage, and access to that data or software complies with the EAR.

## Azure and EAR

If you are subject to the EAR, Azure, Azure Government, and Azure Government Secret can help you meet your EAR compliance requirements.

Except for the Azure region in Hong Kong SAR, Azure datacenters aren't located in proscribed countries or in the Russian Federation. Azure services rely on [FIPS 140](#) validated cryptographic modules in the underlying operating system, and provide you with [many options for encrypting data](#) in transit and at rest, including encryption key management using [Azure Key Vault](#). The Key Vault service can store encryption keys in

FIPS 140 validated hardware security modules (HSMs) under your control, also known as [customer-managed keys \(CMK\)](#). Keys generated inside the Azure Key Vault HSMs aren't exportable – there can be no clear-text version of the key outside the HSMs. This binding is enforced by the underlying HSM. **Azure Key Vault is designed, deployed, and operated such that Microsoft and its agents don't see or extract your cryptographic keys.** For more information, see [How does Azure Key Vault protect your keys?](#)

#### Note

You're responsible for choosing the Azure regions for deploying your applications and data. Moreover, you're responsible for designing your applications to use end-to-end data encryption that meets EAR requirements. Microsoft doesn't inspect, approve, or monitor your Azure applications.

Azure Government provides an extra layer of protection to customers through contractual commitments regarding storage of customer data in the United States and limiting potential access to systems processing customer data to [screened US persons](#).

For more information regarding the EAR, you should review:

- [Azure export controls](#) online documentation
- [Microsoft Azure Export Controls](#) whitepaper

## Applicability

- Azure
- Azure Government
- Azure Government Secret

## Office 365 and EAR

For more information about Office 365 compliance, see [Office 365 EAR documentation](#).

## Frequently asked questions

### What should I do to comply with export control laws when using Azure?

Under the EAR, when data is uploaded to a cloud service, the customer who owns the data — not the cloud services provider — is considered to be the *exporter* who has the responsibility to ensure that transfers, storage, and access to that data or software complies with the EAR. For that reason, you, as the owner of the data, must carefully

assess how your use of the Microsoft cloud may implicate US export controls and determine whether any of the data you want to use or store there may be subject to EAR controls, and if so, what controls apply. To learn more about how Azure can help you ensure your full compliance with US export controls, review the [Microsoft Azure Export Controls](#) whitepaper.

## What technical features does Azure provide to help customers meet their EAR compliance obligations?

The following Azure features are available to you to manage potential export control risks:

- **Ability to control data location** – You have visibility as to where your data is stored, and robust tools to restrict data storage to a single geography, region, or country. For example, you may therefore ensure that data is stored in the United States or your country of choice and minimize transfer of controlled technology/technical data outside the target country. Customer data isn't *intentionally stored* in a non-conforming location, consistent with the EAR rules.
- **Control over access to data** – You can know and control who can access your data and on what terms. Microsoft technical support personnel don't need and don't have default access to customer data. For those rare instances where resolving customer support requests requires elevated access to customer data, [Customer Lockbox for Azure](#) puts you in charge of approving or rejecting customer data access requests.
- **End-to-end encryption** – Implies the data is kept encrypted at all times between the originator and intended recipient, and the means of decryption aren't provided to any third party. Azure relies on [FIPS 140](#) validated cryptographic modules in the underlying operating system, and provides you with [many options for encrypting data](#) in transit and at rest, including encryption key management using [Azure Key Vault](#). The Key Vault service can store encryption keys in FIPS 140 validated hardware security modules (HSMs) under your control, also known as [customer-managed keys \(CMK\)](#). Azure Key Vault is designed, deployed, and operated such that Microsoft and its agents [don't see or extract your cryptographic keys](#).
- **Tools and protocols to prevent unauthorized deemed export/re-export** – Apart from the EAR *end-to-end encryption* safe harbor for physical storage locations, the use of encryption also helps protect against a potential deemed export (or deemed re-export), because even if a non-US person has access to the encrypted data, nothing is actually revealed to non-US person who can't read or understand the data while it is encrypted and thus there is no *release* of any controlled data. Azure offers many encryption capabilities and solutions, flexibility to choose among encryption options, and robust tools for managing encryption.

## **Are Microsoft technologies, products, and services subject to the EAR?**

Most Microsoft technologies, products, and services are either 1) not subject to the EAR and thus aren't on the Commerce Control List and have no ECCN; or 2) they're EAR99 or 5D992 Mass Market-eligible for self-classification by Microsoft and may be exported to non-embargoed countries without a license as No License Required (NLR). That said, a few Microsoft products have been assigned an ECCN that may or may not require a license. For more information, see [Exporting Microsoft Products](#) where you can find exporting information under Product Lookup. Consult the BIS or legal counsel to determine the appropriate license type and eligible countries for export purposes.

## **What's the difference between the EAR and International Traffic in Arms Regulations (ITAR)?**

The primary US export controls with the broadest application are the EAR, administered by the US Department of Commerce. The EAR is applicable to dual-use items that have both commercial and military applications, and to items with purely commercial applications.

The United States also has separate and more specialized export control regulations, such as the ITAR, that governs the most sensitive items and technology. Administered by the US Department of State, ITAR imposes controls on the export, temporary import, re-export, and transfer of many military, defense, and intelligence items – also known as *defense articles* – including related technical data documented on the [United States Munitions List](#) (USML).

## **Should I use Azure or Azure Government for workloads that are subject to EAR?**

You're wholly responsible for ensuring your own compliance with all applicable laws and regulations, and should consult your legal advisor for questions regarding regulatory compliance. Azure and Azure Government have the same security controls in place, including the same provisions for data encryption in transit and at rest to support EAR requirements. The cloud environment decision will rest with you based on your business requirements. Most US government agencies and their partners are best aligned with Azure Government, which provides an additional layer of protection to customers through contractual commitments regarding storage of customer data in the United States and limiting potential access to systems processing customer data to [screened US persons](#).

# **Resources**

- [Azure compliance documentation](#)
- [Azure enables a world of compliance](#)
- [Microsoft 365 compliance offerings](#)

- [What is Azure Government?](#)
- [Explore Azure Government](#)
- [Microsoft government solutions](#)
- [Azure support for export controls](#)
- [Microsoft Azure Export Controls](#) whitepaper
- [Export Administration Regulations](#)
- [Bureau of Industry and Security](#) (BIS)
- [BIS definitions](#)
- [Commerce Control List](#) (CCL)
- [Export Control Classification Number](#) (ECCN)
- [Revisions to Definitions in the Export Administration Regulations](#) - BIS Final Rule published 3 June 2016
- [Supplement No. 1 to Part 740](#) of the EAR

# Federal Risk and Authorization Management Program (FedRAMP)

Article • 04/05/2023

## FedRAMP overview

The US Federal Risk and Authorization Management Program (FedRAMP) was established in December 2011 to provide a standardized approach for assessing, monitoring, and authorizing cloud computing products and services under the Federal Information Security Management Act (FISMA), and to accelerate the adoption of secure cloud solutions by US federal agencies. Cloud Service Providers (CSPs) desiring to sell services to a federal agency can take three paths to demonstrate FedRAMP compliance:

- Earn a Provisional Authorization to Operate (P-ATO) from the FedRAMP Joint Authorization Board (JAB).
- Receive an Authorization to Operate (ATO) from a federal agency.
- Work independently to develop a CSP Supplied Package that meets program requirements.

Each of these paths requires an assessment by an independent third-party assessment organization (3PAO) that is accredited by the program and a stringent technical review by the FedRAMP Program Management Office (PMO).

FedRAMP is based on the National Institute of Standards and Technology (NIST) [SP 800-53](#) standard, augmented by FedRAMP controls and control enhancements. FedRAMP authorizations are granted at three impact levels based on the NIST [FIPS 199](#) guidelines — Low, Moderate, and High. These levels rank the impact that the loss of confidentiality, integrity, or availability could have on an organization — Low (limited effect), Moderate (serious adverse effect), and High (severe or catastrophic effect). The number of controls in the corresponding baseline increases as the impact level increases, for example, FedRAMP Moderate baseline has 325 controls whereas FedRAMP High baseline has 421 controls.

The FedRAMP High authorization represents the highest bar for FedRAMP compliance. The FedRAMP Joint Authorization Board (JAB) is the primary governance and decision-making body for FedRAMP. Representatives from the Department of Defense (DoD), Department of Homeland Security (DHS), and General Services Administration (GSA) serve on the board. The board grants a P-ATO to cloud service offerings (CSO) that have demonstrated FedRAMP compliance. Once a P-ATO is granted, a CSP still requires an authorization (an ATO) from any government agency it works with. A government

agency can use an existing P-ATO in its own security authorization process and rely on it as the basis for issuing an agency ATO that also meets FedRAMP requirements.

 Note

FedRAMP is not a point-in-time certification or accreditation but an assessment and authorization program that comes with provisions for continuous monitoring to ensure that deployed security controls in a CSO remain effective in an evolving threat landscape and changes that occur in the system environment.

## Azure and FedRAMP

Both Azure and Azure Government maintain [FedRAMP High P-ATOs](#) issued by the JAB in addition to more than 400 Moderate and High ATOs issued by individual federal agencies for the in-scope services. And while FedRAMP High authorization in the Azure public cloud will meet the needs of many US government customers, Azure Government provides additional customer assurances through controls that limit potential access to systems processing customer data to [screened US persons](#).

For extra customer assistance, Microsoft provides the Azure Policy regulatory compliance built-in initiatives for Azure and Azure Government, which map to [FedRAMP compliance domains and controls](#):

- Azure
  - [FedRAMP High Azure regulatory compliance built-in initiative](#)
  - [FedRAMP Moderate Azure regulatory compliance built-in initiative](#)
- Azure Government
  - [FedRAMP High Azure Government regulatory compliance built-in initiative](#)
  - [FedRAMP Moderate Azure Government regulatory compliance built-in initiative](#)

Regulatory compliance in Azure Policy provides built-in initiative definitions to view a list of controls and compliance domains based on responsibility – customer, Microsoft, or shared. For Microsoft-responsible controls, we provide extra audit result details based on third-party attestations and our control implementation details to achieve that compliance. Each FedRAMP control is associated with one or more Azure Policy definitions. These policies may help you [assess compliance](#) with the control; however, compliance in Azure Policy is only a partial view of your overall compliance status. Azure Policy helps to enforce organizational standards and assess compliance at scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to more granular status.

# Applicability

- Azure
- Azure Government

## Services in scope

For a list of Microsoft online services in scope for the FedRAMP High P-ATO in Azure and Azure Government, see [Cloud services in audit scope](#).

## Office 365 and FedRAMP

For more information about Office 365 compliance, see [Office 365 FedRAMP documentation](#).

## Attestation documents

You can request Azure and Azure Government FedRAMP documentation directly from the [FedRAMP Marketplace](#) by submitting a package access request form. You must have a .gov or .mil email address to access a FedRAMP security package directly from the FedRAMP Marketplace.

Azure Commercial System Security Plan (SSP) is available from the Service Trust Portal (STP) [FedRAMP reports](#) section. You must sign in to access audit reports on the STP. You must have an existing subscription or free trial account in [Azure](#) or [Azure Government](#) to download audit documents. For more information, see [Get started with Microsoft Service Trust Portal](#).

Select Azure and Azure Government FedRAMP documentation, including the System Security Plan (SSP), continuous monitoring reports, Plan of Action and Milestones (POA&M), and so on, are available under NDA and pending access authorization from a restricted Service Trust Portal (STP) [FedRAMP reports](#) section. Contact your Microsoft account representative for assistance.

## Azure penetration test reports

An independent third-party assessment organization (3PAO) that is accredited by FedRAMP conducts Azure penetration tests annually. The resulting reports are typically due in September for submission to the FedRAMP Joint Authorization Board (JAB). Once reviewed and approved by the FedRAMP JAB, penetration test reports are uploaded to

the Service Trust Portal (STP) [Pen Tests and Security Assessments](#) section. This process can take several months from report submission. Therefore, if you can't locate the Azure penetration test report for the current year, it's most likely still under review and pending approval. We aim to upload penetration test reports to the STP by December or shortly thereafter; however, this timeline can vary.

If any vulnerabilities are identified in penetration test reports, their resolution can be tracked via Plan of Action and Milestones (POA&M) submissions. Contact your Microsoft account representative for assistance with access to a restricted section of the STP from where you can download select FedRAMP documentation, including the POA&M files.

For penetration testing that Microsoft conducts routinely on the Azure cloud services platform, see *Live-site penetration testing* in [Security assurance processes and practices](#). For penetration testing that you can conduct on your own cloud applications, see [Penetration testing](#).

## Frequently asked questions

### Which Azure regions are in scope for the FedRAMP High P-ATO?

All Azure public regions in the United States are in scope for the Azure FedRAMP High P-ATO. Azure regions outside the United States aren't formally authorized by the FedRAMP JAB, and aren't in the FedRAMP High P-ATO scope. However, Azure security controls and operational processes are the same everywhere Azure runs. FedRAMP is based on the NIST SP 800-53 control baselines. All NIST SP 800-53 controls that support the Azure FedRAMP High P-ATO in the United States are also operational in other Azure regions outside the United States. Therefore, Azure customers outside the United States can count on the same control implementation details that pertain to the NIST SP 800-53 High control baseline.

### Which Azure Government regions are in scope for the FedRAMP High P-ATO?

Azure Government regions US Gov Arizona, US Gov Texas, and US Gov Virginia are in scope for the Azure Government FedRAMP High P-ATO.

### Does Azure comply with the Federal Information Security Management Act (FISMA)?

FISMA is a US federal law that requires US federal agencies and their partners to procure information systems and services only from organizations that adhere to FISMA requirements. Most agencies and their vendors that indicate that they are FISMA-compliant are referring to how they meet the controls identified in NIST SP 800-53. The FISMA process (but not the underlying standards) was replaced by FedRAMP in 2011. FedRAMP provides a standardized approach for security assessment, authorization, and continuous monitoring of cloud services.

## To whom does FedRAMP apply?

FedRAMP is mandatory for federal agency cloud deployments and service models at the low, moderate, and high-risk impact levels. Any federal agency that wants to engage a CSP may be required to meet FedRAMP specifications. In addition, companies that employ cloud technologies in products or services used by the federal government may be required to obtain an ATO.

## Where does my agency start its own compliance effort?

For an overview of the steps federal agencies must take to successfully navigate FedRAMP and meet its requirements, go to [Get Authorized: Agency Authorization](#).

## Can I use Azure FedRAMP compliance in my agency's authorization process?

Yes. You may use Azure or Azure Government FedRAMP High P-ATO as the foundation for any program or initiative that requires an ATO from a federal government agency. However, you need to achieve your own authorizations for components outside these services.

## Where can I get the Azure FedRAMP documentation?

For links to audit documentation, see [Attestation documents](#). You must sign in to access audit reports on the Service Trust Portal (STP). For more information, see [Get started with Microsoft Service Trust Portal](#). You must have an existing subscription or free trial account in [Azure](#) or [Azure Government](#) to download audit reports from the STP.

## What was the resolution of identified vulnerabilities and where is the latest Azure penetration test report?

See [Azure penetration test reports](#) for more information.

## What Azure Government services are covered by FedRAMP High P-ATO and in what regions?

To find out what services are available in Azure Government, see [Products available by region](#). For a list of services in scope for the FedRAMP High P-ATO, see [Cloud services in audit scope](#).

# Resources

- [Azure compliance documentation](#)
- [Azure enables a world of compliance](#)
- [Microsoft 365 compliance offerings](#)
- [Compliance on the Microsoft Trust Center](#)
- [What is Azure Government?](#)
- [Explore Azure Government](#)
- [Microsoft government solutions](#)

- FedRAMP documents and templates ↗
- NIST SP 800-53 ↗ *Security and Privacy Controls for Information Systems and Organizations*

# Details of the FedRAMP High Regulatory Compliance built-in initiative

Article • 01/02/2024

The following article details how the Azure Policy Regulatory Compliance built-in initiative definition maps to **compliance domains** and **controls** in FedRAMP High. For more information about this compliance standard, see [FedRAMP High](#). To understand *Ownership*, see [Azure Policy policy definition](#) and [Shared responsibility in the cloud](#).

The following mappings are to the FedRAMP High controls. Many of the controls are implemented with an [Azure Policy](#) initiative definition. To review the complete initiative definition, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **FedRAMP High** Regulatory Compliance built-in initiative definition.

## ⓘ Important

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policy definitions themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between compliance domains, controls, and Azure Policy definitions for this compliance standard may change over time. To view the change history, see the [GitHub Commit History](#).

## Access Control

### Access Control Policy And Procedures

ID: FedRAMP High AC-1 Ownership: Shared

ⓘ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review access control policies and procedures ↗	CMA_0457 - Review access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Account Management

ID: FedRAMP High AC-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
A maximum of 3 owners should be designated for your subscription ↗	It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
An Azure Active Directory administrator should be provisioned for SQL servers ↗	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
App Service apps should use managed identity ↗	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Assign account managers ↗	CMA_0015 - Assign account managers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Audit usage of custom RBAC roles ↗	Audit built-in roles such as 'Owner, Contributer, Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and	Audit, Disabled	<a href="#">1.0.1 ↗</a>

<b>Name</b>  (Azure portal)	<b>Description</b>	<b>Effect(s)</b>	<b>Version</b>  (GitHub)
	requires a rigorous review and threat modeling		
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	1.1.0 ↗
<a href="#">Blocked accounts with owner permissions on Azure resources should be removed ↗</a>	Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in.	AuditIfExists, Disabled	1.0.0 ↗
<a href="#">Blocked accounts with read and write permissions on Azure resources should be removed ↗</a>	Deprecated accounts should be removed from your subscriptions. Deprecated accounts are accounts that have been blocked from signing in.	AuditIfExists, Disabled	1.0.0 ↗
<a href="#">Cognitive Services accounts should have local authentication methods disabled ↗</a>	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
<a href="#">Define and enforce conditions for shared and group accounts ↗</a>	CMA_0117 - Define and enforce conditions for shared and group accounts	Manual, Disabled	1.1.0 ↗
<a href="#">Define information system account types ↗</a>	CMA_0121 - Define information system account types	Manual, Disabled	1.1.0 ↗
<a href="#">Document access privileges ↗</a>	CMA_0186 - Document access privileges	Manual, Disabled	1.1.0 ↗
<a href="#">Establish conditions for role membership ↗</a>	CMA_0269 - Establish conditions for role membership	Manual, Disabled	1.1.0 ↗
<a href="#">Function apps should use managed identity ↗</a>	Use a managed identity for enhanced authentication security	AuditIfExists, Disabled	3.0.0 ↗
<a href="#">Guest accounts with owner permissions on Azure resources should be removed ↗</a>	External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.	AuditIfExists, Disabled	1.0.0 ↗
<a href="#">Guest accounts with read permissions on</a>	External accounts with read privileges should be removed from your subscription in order to prevent unmonitored access.	AuditIfExists, Disabled	1.0.0 ↗

Azure resources Name <a href="#">should be removed ↴ (Azure portal)</a>	Description	Effect(s)	Version (GitHub)
Guest accounts with write permissions on Azure resources should be removed ↴	External accounts with write privileges should be removed from your subscription in order to prevent unmonitored access.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Monitor account activity ↴	CMA_0377 - Monitor account activity	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Notify Account Managers of customer controlled accounts ↴	CMA_C1009 - Notify Account Managers of customer controlled accounts	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Reissue authenticators for changed groups and accounts ↴	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Require approval for account creation ↴	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Restrict access to privileged accounts ↴	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review account provisioning logs ↴	CMA_0460 - Review account provisioning logs	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review user accounts ↴	CMA_0480 - Review user accounts	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Service Fabric clusters should only use Azure Active Directory for client authentication ↴	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	<a href="#">1.1.0 ↴</a>

## Automated System Account Management

ID: FedRAMP High AC-2 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An Azure Active Directory	Audit provisioning of an Azure Active Directory administrator for your SQL server	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
administrator should be provisioned for SQL servers ↗	to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services		
Automate account management ↗	CMA_0026 - Automate account management	Manual, Disabled	1.1.0 ↗
Cognitive Services accounts should have local authentication methods disabled ↗	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> .	Audit, Deny, Disabled	1.0.0 ↗
Manage system and admin accounts ↗	CMA_0368 - Manage system and admin accounts	Manual, Disabled	1.1.0 ↗
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	1.1.0 ↗
Notify when account is not needed ↗	CMA_0383 - Notify when account is not needed	Manual, Disabled	1.1.0 ↗
Service Fabric clusters should only use Azure Active Directory for client authentication ↗	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	1.1.0 ↗

## Disable Inactive Accounts

ID: FedRAMP High AC-2 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	1.1.0 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗

## Automated Audit Actions

ID: FedRAMP High AC-2 (4) Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate account management ↗</a>	CMA_0026 - Automate account management	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage system and admin accounts ↗</a>	CMA_0368 - Manage system and admin accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Monitor access across the organization ↗</a>	CMA_0376 - Monitor access across the organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Notify when account is not needed ↗</a>	CMA_0383 - Notify when account is not needed	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Inactivity Logout

ID: FedRAMP High AC-2 (5) Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define and enforce inactivity log policy ↗</a>	CMA_C1017 - Define and enforce inactivity log policy	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Role-Based Schemes

ID: FedRAMP High AC-2 (7) Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An Azure Active Directory administrator should be provisioned for SQL servers ↗	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	1.0.0 ↗
Audit privileged functions ↗	CMA_0019 - Audit privileged functions	Manual, Disabled	1.1.0 ↗
Audit usage of custom RBAC roles ↗	Audit built-in roles such as 'Owner', 'Contributer', 'Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling	Audit, Disabled	1.0.1 ↗
Cognitive Services accounts should have local authentication methods disabled ↗	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
Monitor account activity ↗	CMA_0377 - Monitor account activity	Manual, Disabled	1.1.0 ↗
Monitor privileged role assignment ↗	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	1.1.0 ↗
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	1.1.0 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗
Service Fabric clusters should only use Azure Active Directory for client authentication ↗	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	1.1.0 ↗
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↗

## Restrictions On Use Of Shared Groups / Accounts

ID: FedRAMP High AC-2 (9) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define and enforce conditions for shared and group accounts ↗</a>	CMA_0117 - Define and enforce conditions for shared and group accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Shared / Group Account Credential Termination

ID: FedRAMP High AC-2 (10) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Terminate customer controlled account credentials ↗</a>	CMA_C1022 - Terminate customer controlled account credentials	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Usage Conditions

ID: FedRAMP High AC-2 (11) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Enforce appropriate usage of all accounts ↗</a>	CMA_C1023 - Enforce appropriate usage of all accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Account Monitoring / Atypical Usage

ID: FedRAMP High AC-2 (12) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .	AuditIfNotExists, Disabled	6.0.0- preview ↗
Azure Defender for App Service should be enabled ↗	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Azure SQL Database servers should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for DNS should be enabled ↗	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for Key Vault should be enabled ↗	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Resource Manager	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
should be enabled ↗	about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for SQL servers on machines should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↗
Management ports of virtual machines should be protected with just-in-time network access control ↗	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.0.0 ↗
Microsoft Defender for Containers should be enabled ↗	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	1.0.0 ↗
Microsoft Defender for Storage	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
should be enabled ↗	workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.		
Monitor account activity ↗	CMA_0377 - Monitor account activity	Manual, Disabled	1.1.0 ↗
Report atypical behavior of user accounts ↗	CMA_C1025 - Report atypical behavior of user accounts	Manual, Disabled	1.1.0 ↗

## Disable Accounts For High-Risk Individuals

ID: FedRAMP High AC-2 (13) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Disable user accounts posing a significant risk ↗	CMA_C1026 - Disable user accounts posing a significant risk	Manual, Disabled	1.1.0 ↗

## Access Enforcement

ID: FedRAMP High AC-3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Accounts with owner permissions on Azure resources	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should be MFA enabled ↗</a>			
<a href="#">Accounts with read permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Accounts with write permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗ .	modify	<a href="#">4.0.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗ .	modify	<a href="#">4.0.0 ↗</a>
<a href="#">An Azure Active Directory administrator should be provisioned for SQL servers ↗</a>	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">App Service apps should use</a>	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name	Description	Effect(s)	Version
<a href="#">Audit Linux machines that have accounts without passwords</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Linux machines that have accounts without passwords	AuditIfNotExists, Disabled	(GitHub) <a href="#">5.0.0</a>
<a href="#">Authentication to Linux machines should require SSH keys</a>	Although SSH itself provides an encrypted connection, using passwords with SSH still leaves the VM vulnerable to brute-force attacks. The most secure option for authenticating to an Azure Linux virtual machine over SSH is with a public-private key pair, also known as SSH keys. Learn more: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed">https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed</a> .	AuditIfNotExists, Disabled	<a href="#">3.1.0</a>
<a href="#">Authorize access to security functions and information</a>	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0</a>
<a href="#">Authorize and manage access</a>	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0</a>
<a href="#">Cognitive Services accounts should have local authentication methods disabled</a>	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> .	Audit, Deny, Disabled	<a href="#">1.0.0</a>
<a href="#">Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs</a>	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	<a href="#">3.0.0</a>
<a href="#">Enforce logical access</a>	CMA_0245 - Enforce logical access	Manual, Disabled	<a href="#">1.1.0</a>
<a href="#">Enforce mandatory and discretionary</a>	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
access control policies ↗			
Function apps should use managed identity ↗	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	3.0.0 ↗
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	1.1.0 ↗
Review user groups and applications with access to sensitive data ↗	CMA_0481 - Review user groups and applications with access to sensitive data	Manual, Disabled	1.1.0 ↗
Service Fabric clusters should only use Azure Active Directory for client authentication ↗	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	1.1.0 ↗
Storage accounts should be migrated to new Azure Resource Manager resources ↗	Use new Azure Resource Manager for your storage accounts to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management	Audit, Deny, Disabled	1.0.0 ↗
Virtual machines should be migrated to new Azure Resource Manager resources ↗	Use new Azure Resource Manager for your virtual machines to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management	Audit, Deny, Disabled	1.0.0 ↗

# Information Flow Enforcement

ID: FedRAMP High AC-4 Ownership: Shared

 Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
[Preview]: All Internet traffic should be routed via your deployed Azure Firewall ↗	Azure Security Center has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall	AuditIfNotExists, Disabled	3.0.0-preview ↗
[Preview]: Storage account public access should be disallowed ↗	Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it.	audit, Audit, deny, Deny, disabled, Disabled	3.1.0-preview ↗
Adaptive network hardening recommendations should be applied on internet facing virtual machines ↗	Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface	AuditIfNotExists, Disabled	3.0.0 ↗
All network ports should be restricted on network security groups associated to your virtual machine ↗	Azure Security Center has identified some of your network security groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.	AuditIfNotExists, Disabled	3.0.0 ↗
API Management services should use a virtual network ↗	Azure Virtual Network deployment provides enhanced security, isolation and allows you to place your API Management service in a non-internet routable network that you control access to. These networks can then be connected to your on-premises networks using various VPN technologies, which enables access to your	Audit, Deny, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	backend services within the network and/or on-premises. The developer portal and API gateway, can be configured to be accessible either from the Internet or only within the virtual network.		
App Configuration should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> ↗ .	AuditIfNotExists, Disabled	1.0.2 ↗
App Service apps should not have CORS configured to allow every resource to access your apps ↗	Cross-Origin Resource Sharing (CORS) should not allow all domains to access your app. Allow only required domains to interact with your app.	AuditIfNotExists, Disabled	2.0.0 ↗
Authorized IP ranges should be defined on Kubernetes Services ↗	Restrict access to the Kubernetes Service Management API by granting API access only to IP addresses in specific ranges. It is recommended to limit access to authorized IP ranges to ensure that only applications from allowed networks can access the cluster.	Audit, Disabled	2.0.1 ↗
Azure API for FHIR should use private link ↗	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> ↗ .	Audit, Disabled	1.0.0 ↗
Azure Cache for Redis should use private link ↗	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances,	AuditIfNotExists, Disabled	1.0.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
	<p>data leakage risks are reduced. Learn more at:  <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a>.</p>		
<a href="#">Azure Cognitive Search service should use a SKU that supports private link ↗</a>	<p>With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at:  <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.</p>	Audit, Deny, Disabled	1.0.0 ↗
<a href="#">Azure Cognitive Search services should disable public network access ↗</a>	<p>Disabling public network access improves security by ensuring that your Azure Cognitive Search service is not exposed on the public internet. Creating private endpoints can limit exposure of your Search service. Learn more at:  <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.</p>	Audit, Deny, Disabled	1.0.0 ↗
<a href="#">Azure Cognitive Search services should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at:  <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.</p>	Audit, Disabled	1.0.0 ↗
<a href="#">Azure Cosmos DB accounts should have firewall rules ↗</a>	<p>Firewall rules should be defined on your Azure Cosmos DB accounts to prevent traffic from unauthorized sources.  Accounts that have at least one IP rule defined with the virtual network filter enabled are deemed compliant. Accounts</p>	Audit, Deny, Disabled	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	disabling public access are also deemed compliant.		
Azure Data Factory should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Event Grid domains should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> .	Audit, Disabled	1.0.2 ↗
Azure Event Grid topics should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> .	Audit, Disabled	1.0.2 ↗
Azure File Sync should use private link ↗	Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.		
Azure Key Vault should have firewall enabled ↗	Enable the key vault firewall so that the key vault is not accessible by default to any public IPs. Optionally, you can configure specific IP ranges to limit access to those networks. Learn more at: <a href="https://docs.microsoft.com/azure/key-vault/general/network-security">https://docs.microsoft.com/azure/key-vault/general/network-security</a>	Audit, Deny, Disabled	3.2.1 ↗
Azure Key Vaults should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink</a> .	[parameters('audit_effect')]	1.2.1 ↗
Azure Machine Learning workspaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .	Audit, Disabled	1.0.0 ↗
Azure Service Bus namespaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at:	AuditIfExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p><a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a>.</p>		
Azure SignalR Service should use private link ↗	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at:</p> <p><a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .</p>	Audit, Disabled	1.0.0 ↗
Azure Synapse workspaces should use private link ↗	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at:</p> <p><a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a>.</p>	Audit, Disabled	1.0.1 ↗
Azure Web PubSub Service should use private link ↗	<p>Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks.</p> <p>Learn more about private links at:</p> <p><a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a> .</p>	Audit, Disabled	1.0.0 ↗
Cognitive Services accounts should disable public network access ↗	<p>To improve the security of Cognitive Services accounts, ensure that it isn't exposed to the public internet and can only be accessed from a private endpoint. Disable the public network access property</p>	Audit, Deny, Disabled	3.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	as described in <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> . This option disables access from any public address space outside the Azure IP range, and denies all logins that match IP or virtual network-based firewall rules. This reduces data leakage risks.		
<a href="#">Cognitive Services accounts should restrict network access ↗</a>	Network access to Cognitive Services accounts should be restricted. Configure network rules so only applications from allowed networks can access the Cognitive Services account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges.	Audit, Deny, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Cognitive Services should use private link ↗</a>	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage.  Learn more about private links at: <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> .	Audit, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Container registries should not allow unrestricted network access ↗</a>	Azure container registries by default accept connections over the internet from hosts on any network. To protect your registries from potential threats, allow access from only specific private endpoints, public IP addresses or address ranges. If your registry doesn't have network rules configured, it will appear in the unhealthy resources. Learn more about Container Registry network rules here:  <a href="https://aka.ms/acr/privatelink">https://aka.ms/acr/privatelink</a> , <a href="https://aka.ms/acr/portal/public-network">https://aka.ms/acr/portal/public-network</a> and <a href="https://aka.ms/acr/vnet">https://aka.ms/acr/vnet</a> .	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Container registries should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a> .	Audit, Disabled	1.0.1 ↗
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	1.1.0 ↗
CosmosDB accounts should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a> .	Audit, Disabled	1.0.0 ↗
Disk access resources should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Employ flow control mechanisms of encrypted information ↗	CMA_0211 - Employ flow control mechanisms of encrypted information	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Event Hub namespaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Internet-facing virtual machines should be protected with network security groups ↗	Protect your virtual machines from potential threats by restricting access to them with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsg-doc">https://aka.ms/nsg-doc</a> ↗	AuditIfNotExists, Disabled	3.0.0 ↗
IoT Hub device provisioning service instances should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a> ↗ .	Audit, Disabled	1.0.0 ↗
IP Forwarding on your virtual machine should be disabled ↗	Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely required (e.g., when using the VM as a network virtual appliance), and therefore, this should be reviewed by the network security team.	AuditIfNotExists, Disabled	3.0.0 ↗
Management ports of virtual machines should be protected with just-in-time network access control ↗	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Management ports should be closed on your virtual machines ↗	Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine.	AuditIfNotExists, Disabled	3.0.0 ↗
Non-internet-facing virtual machines should be protected with network security groups ↗	Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsgr-doc">https://aka.ms/nsgr-doc</a> ↗	AuditIfNotExists, Disabled	3.0.0 ↗
Private endpoint connections on Azure SQL Database should be enabled ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↗
Private endpoint should be enabled for MariaDB servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for MySQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for PostgreSQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Public network access on Azure SQL Database should be disabled ↗	Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP or virtual network based firewall rules.	Audit, Deny, Disabled	1.1.0 ↗
Public network access should be disabled for MariaDB servers ↗	Disable the public network access property to improve security and ensure your Azure Database for MariaDB can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↗
Public network access should be disabled for MySQL servers ↗	Disable the public network access property to improve security and ensure your Azure Database for MySQL can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↗
Public network access should be disabled for PostgreSQL servers ↗	Disable the public network access property to improve security and ensure your Azure Database for PostgreSQL can only be accessed from a private endpoint. This configuration disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.1 ↗
Storage accounts should restrict network access ↗	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges	Audit, Deny, Disabled	1.1.1 ↗
Storage accounts should restrict network access	Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering	Audit, Deny, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">using virtual network rules ↗</a>	prevents public IPs from accessing your storage accounts.		
<a href="#">Storage accounts should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview</a> ↗	AuditIfNotExists, Disabled	2.0.0 ↗
<a href="#">Subnets should be associated with a Network Security Group ↗</a>	Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.	AuditIfNotExists, Disabled	3.0.0 ↗
<a href="#">VM Image Builder templates should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .	Audit, Disabled, Deny	1.1.0 ↗

## Security Policy Filters

ID: FedRAMP High AC-4 (8) Ownership: Shared

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Information flow control using security policy filters ↗</a>	CMA_C1029 - Information flow control using security policy filters	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Physical / Logical Separation Of Information Flows

ID: FedRAMP High AC-4 (21) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control information flow ↗</a>	CMA_0079 - Control information flow	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish firewall and router configuration standards ↗</a>	CMA_0272 - Establish firewall and router configuration standards	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish network segmentation for card holder data environment ↗</a>	CMA_0273 - Establish network segmentation for card holder data environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify and manage downstream information exchanges ↗</a>	CMA_0298 - Identify and manage downstream information exchanges	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Separation Of Duties

ID: FedRAMP High AC-5 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define access authorizations to support separation of duties ↗</a>	CMA_0116 - Define access authorizations to support separation of duties	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document separation of duties ↗</a>	CMA_0204 - Document separation of duties	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Separate duties of individuals ↗</a>	CMA_0492 - Separate duties of individuals	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">There should be more than one owner assigned to your subscription ↗</a>	It is recommended to designate more than one subscription owner in order to have administrator access redundancy.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Least Privilege

ID: FedRAMP High AC-6 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">A maximum of 3 owners should be designated for your subscription ↗</a>	It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Audit usage of custom RBAC roles ↗</a>	Audit built-in roles such as 'Owner', 'Contributer', 'Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Design an access control model ↗</a>	CMA_0129 - Design an access control model	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ least privilege access ↗</a>	CMA_0212 - Employ least privilege access	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Authorize Access To Security Functions

ID: FedRAMP High AC-6 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authorize access to security functions and information ↗</a>	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authorize and manage access ↗</a>	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce mandatory and discretionary access control policies ↗</a>	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Privileged Accounts

ID: FedRAMP High AC-6 (5) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Restrict access to privileged accounts ↗</a>	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Review Of User Privileges

ID: FedRAMP High AC-6 (7) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">A maximum of 3 owners should be designated for your subscription ↗</a>	It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Audit usage of custom RBAC roles ↗</a>	Audit built-in roles such as 'Owner, Contributer, Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Reassign or remove user privileges as needed ↗</a>	CMA_C1040 - Reassign or remove user privileges as needed	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">Review user privileges ↗</a>	CMA_C1039 - Review user privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Privilege Levels For Code Execution

ID: FedRAMP High AC-6 (8) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">Enforce software execution privileges ↗</a>	CMA_C1041 - Enforce software execution privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Auditing Use Of Privileged Functions

ID: FedRAMP High AC-6 (9) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">Audit privileged functions ↗</a>	CMA_0019 - Audit privileged functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct a full text analysis of logged privileged commands ↗</a>	CMA_0056 - Conduct a full text analysis of logged privileged commands	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Monitor privileged role assignment ↗</a>	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Restrict access to privileged accounts ↗</a>	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Revoke privileged roles as appropriate ↗</a>	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Use privileged identity management ↗</a>	CMA_0533 - Use privileged identity management	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Unsuccessful Logon Attempts

ID: FedRAMP High AC-7 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Enforce a limit of consecutive failed login attempts ↗</a>	CMA_C1044 - Enforce a limit of consecutive failed login attempts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Concurrent Session Control

ID: FedRAMP High AC-10 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define and enforce the limit of concurrent sessions ↗</a>	CMA_C1050 - Define and enforce the limit of concurrent sessions	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Session Termination

ID: FedRAMP High AC-12 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Terminate user session automatically ↗</a>	CMA_C1054 - Terminate user session automatically	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## User-Initiated Logouts / Message Displays

ID: FedRAMP High AC-12 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Display an explicit logout message ↗	CMA_C1056 - Display an explicit logout message	Manual, Disabled	1.1.0 ↗
Provide the logout capability ↗	CMA_C1055 - Provide the logout capability	Manual, Disabled	1.1.0 ↗

## Permitted Actions Without Identification Or Authentication

ID: FedRAMP High AC-14 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Identify actions allowed without authentication ↗	CMA_0295 - Identify actions allowed without authentication	Manual, Disabled	1.1.0 ↗

## Remote Access

ID: FedRAMP High AC-17 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	modify	4.0.0 ↗
Add system-assigned	This policy adds a system-assigned managed identity to virtual machines	modify	4.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↳	hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↳.		
App Configuration should use private link ↳	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> ↳.	AuditIfNotExists, Disabled	1.0.2 ↳
App Service apps should have remote debugging turned off ↳	Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0 ↳
Audit Linux machines that allow remote connections from accounts without passwords ↳	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↳. Machines are non-compliant if Linux machines that allow remote connections from accounts without passwords	AuditIfNotExists, Disabled	3.0.0 ↳
Authorize remote access ↳	CMA_0024 - Authorize remote access	Manual, Disabled	1.1.0 ↳
Azure API for FHIR should	Azure API for FHIR should have at least one approved private endpoint connection.	Audit, Disabled	1.0.0 ↳

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">use private link ↗</a>	Clients in a virtual network can securely access resources that have private endpoint connections through private links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> .		
<a href="#">Azure Cache for Redis should use private link ↗</a>	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Cognitive Search service should use a SKU that supports private link ↗</a>	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Cognitive Search services should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Data Factory should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a>.</p>		
<a href="#">Azure Event Grid domains should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a>.</p>	Audit, Disabled	1.0.2 ↗
<a href="#">Azure Event Grid topics should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a>.</p>	Audit, Disabled	1.0.2 ↗
<a href="#">Azure File Sync should use private link ↗</a>	<p>Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.</p>	AuditIfExists, Disabled	1.0.0 ↗
<a href="#">Azure Key Vaults should</a>	<p>Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or</p>	[parameters('audit_effect')]	1.2.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">use private link ↗</a>	destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink</a> .		
<a href="#">Azure Machine Learning workspaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .	Audit, Disabled	1.0.0 ↗
<a href="#">Azure Service Bus namespaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
<a href="#">Azure SignalR Service should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Spring Cloud should use network injection ↗	Azure Spring Cloud instances should use virtual network injection for the following purposes: 1. Isolate Azure Spring Cloud from Internet. 2. Enable Azure Spring Cloud to interact with systems in either on premises data centers or Azure service in other virtual networks. 3. Empower customers to control inbound and outbound network communications for Azure Spring Cloud.	Audit, Disabled, Deny	1.2.0 ↗
Azure Synapse workspaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a> .	Audit, Disabled	1.0.1 ↗
Azure Web PubSub Service should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a> ↗.	Audit, Disabled	1.0.0 ↗
Cognitive Services should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage. Learn more about private links at:	Audit, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> .		
Container registries should use private link ↴	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a> .	Audit, Disabled	1.0.1 ↴
CosmosDB accounts should use private link ↴	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a> .	Audit, Disabled	1.0.0 ↴
Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↴	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	3.0.0 ↴
Deploy the Windows Guest Configuration extension to enable Guest Configuration	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be	deployIfNotExists	1.2.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
assignments on Windows VMs ↗	deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .		
Disk access resources should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Document mobility training ↗	CMA_0191 - Document mobility training	Manual, Disabled	1.1.0 ↗
Document remote access guidelines ↗	CMA_0196 - Document remote access guidelines	Manual, Disabled	1.1.0 ↗
Event Hub namespaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Function apps should have remote debugging turned off ↗	Remote debugging requires inbound ports to be opened on Function apps. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0 ↗
Implement controls to secure	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
alternate work sites ↗			
IoT Hub device provisioning service instances should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a> ↗.	Audit, Disabled	1.0.0 ↗
Private endpoint connections on Azure SQL Database should be enabled ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↗
Private endpoint should be enabled for MariaDB servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for MySQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for PostgreSQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and	AuditIfNotExists, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	prevent access from all other IP addresses, including within Azure.		
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗
Storage accounts should restrict network access ↗	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges	Audit, Deny, Disabled	1.1.1 ↗
Storage accounts should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview</a> ↗	AuditIfNotExists, Disabled	2.0.0 ↗
VM Image Builder templates should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .	Audit, Disabled, Deny	1.1.0 ↗

## Automated Monitoring / Control

ID: FedRAMP High AC-17 (1) Ownership: Shared

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	4.0.0 ↗
Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	4.0.0 ↗
App Configuration should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> .	AuditIfNotExists, Disabled	1.0.2 ↗
App Service apps should have remote debugging turned off ↗	Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit Linux machines that allow remote connections from accounts without passwords ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Linux machines that allow remote connections from accounts without passwords	AuditIfNotExists, Disabled	3.0.0 ↗
Azure API for FHIR should use private link ↗	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> ↗.	Audit, Disabled	1.0.0 ↗
Azure Cache for Redis should use private link ↗	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Cognitive Search service should use a SKU that supports private link ↗	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints ↗</a> .		
Azure Data Factory should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Event Grid domains should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints ↗</a> .	Audit, Disabled	1.0.2 ↗
Azure Event Grid topics should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints ↗</a> .	Audit, Disabled	1.0.2 ↗
Azure File Sync should	Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">use private link ↗</a>	Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.		
<a href="#">Azure Key Vaults should use private link ↗</a>	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink</a> .	[parameters('audit_effect')]	<a href="#">1.2.1 ↗</a>
<a href="#">Azure Machine Learning workspaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .	Audit, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Service Bus namespaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .	AuditIfNotExist, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure SignalR Service should</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or	Audit, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">use private link ↗</a>	destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .		
<a href="#">Azure Spring Cloud should use network injection ↗</a>	Azure Spring Cloud instances should use virtual network injection for the following purposes: 1. Isolate Azure Spring Cloud from Internet. 2. Enable Azure Spring Cloud to interact with systems in either on premises data centers or Azure service in other virtual networks. 3. Empower customers to control inbound and outbound network communications for Azure Spring Cloud.	Audit, Disabled, Deny	<a href="#">1.2.0 ↗</a>
<a href="#">Azure Synapse workspaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a> .	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Azure Web PubSub Service should use private link ↗</a>	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a> .	Audit, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Cognitive Services should use private link ↗</a>	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage. Learn more about private links at: <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> ↗.	Audit, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Container registries should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a> ↗.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">CosmosDB accounts should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a> .	Audit, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↗</a>	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition.	deployIfNotExists	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .		
Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	1.2.0
Disk access resources should use private link	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a> .	AuditIfNotExists, Disabled	1.0.0
Event Hub namespaces should use private link	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0
Function apps should have remote debugging turned off	Remote debugging requires inbound ports to be opened on Function apps. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0
IoT Hub device provisioning	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or	Audit, Disabled	1.0.0

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
service instances should use private link ↴	destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a> .		
Monitor access across the organization ↴	CMA_0376 - Monitor access across the organization	Manual, Disabled	1.1.0 ↴
Private endpoint connections on Azure SQL Database should be enabled ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↴
Private endpoint should be enabled for MariaDB servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↴
Private endpoint should be enabled for MySQL servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↴
Private endpoint should be enabled for PostgreSQL servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and	AuditIfNotExists, Disabled	1.0.2 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	prevent access from all other IP addresses, including within Azure.		
Storage accounts should restrict network access <a href="#">↗</a>	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges	Audit, Deny, Disabled	1.1.1 <a href="#">↗</a>
Storage accounts should use private link <a href="#">↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview</a> <a href="#">↗</a>	AuditIfNotExists, Disabled	2.0.0 <a href="#">↗</a>
VM Image Builder templates should use private link <a href="#">↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .	Audit, Disabled, Deny	1.1.0 <a href="#">↗</a>

## Protection Of Confidentiality / Integrity Using Encryption

ID: FedRAMP High AC-17 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Notify users of system logon or access ↗	CMA_0382 - Notify users of system logon or access	Manual, Disabled	1.1.0 ↗
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗

## Managed Access Control Points

ID: FedRAMP High AC-17 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	1.1.0 ↗

## Privileged Commands / Access

ID: FedRAMP High AC-17 (4) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize remote access ↗	CMA_0024 - Authorize remote access	Manual, Disabled	1.1.0 ↗
Authorize remote access to privileged commands ↗	CMA_C1064 - Authorize remote access to privileged commands	Manual, Disabled	1.1.0 ↗
Document remote access guidelines ↗	CMA_0196 - Document remote access guidelines	Manual, Disabled	1.1.0 ↗
Implement controls to secure alternate work sites ↗	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	1.1.0 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗

## Disconnect / Disable Access

ID: FedRAMP High AC-17 (9) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide capability to disconnect or disable remote access ↗	CMA_C1066 - Provide capability to disconnect or disable remote access	Manual, Disabled	1.1.0 ↗

## Wireless Access

ID: FedRAMP High AC-18 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document and implement wireless access guidelines ↗	CMA_0190 - Document and implement wireless access guidelines	Manual, Disabled	1.1.0 ↗
Protect wireless access ↗	CMA_0411 - Protect wireless access	Manual, Disabled	1.1.0 ↗

## Authentication And Encryption

ID: FedRAMP High AC-18 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document and implement wireless access guidelines ↗	CMA_0190 - Document and implement wireless access guidelines	Manual, Disabled	1.1.0 ↗
Identify and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	1.1.0 ↗
Protect wireless access ↗	CMA_0411 - Protect wireless access	Manual, Disabled	1.1.0 ↗

## Access Control For Mobile Devices

ID: FedRAMP High AC-19 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define mobile device requirements ↗</a>	CMA_0122 - Define mobile device requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Full Device / Container-Based Encryption

ID: FedRAMP High AC-19 (5) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define mobile device requirements ↗</a>	CMA_0122 - Define mobile device requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Protect data in transit using encryption ↗</a>	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Use Of External Information Systems

ID: FedRAMP High AC-20 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish terms and conditions for accessing resources ↗</a>	CMA_C1076 - Establish terms and conditions for accessing resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish terms and conditions for processing resources ↗</a>	CMA_C1077 - Establish terms and conditions for processing resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Limits On Authorized Use

ID: FedRAMP High AC-20 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Verify security controls for external information systems ↗</a>	CMA_0541 - Verify security controls for external information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Portable Storage Devices

ID: FedRAMP High AC-20 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Block untrusted and unsigned processes that run from USB ↗</a>	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Control use of portable storage devices ↗</a>	CMA_0083 - Control use of portable storage devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information Sharing

ID: FedRAMP High AC-21 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Automate information sharing decisions ↗</a>	CMA_0028 - Automate information sharing decisions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Facilitate information sharing ↗</a>	CMA_0284 - Facilitate information sharing	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Publicly Accessible Content

ID: FedRAMP High AC-22 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Designate authorized personnel to post publicly accessible information ↗</a>	CMA_C1083 - Designate authorized personnel to post publicly accessible information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review content prior to posting publicly accessible information ↗</a>	CMA_C1085 - Review content prior to posting publicly accessible information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review publicly accessible content for nonpublic information ↗</a>	CMA_C1086 - Review publicly accessible content for nonpublic information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Train personnel on disclosure of nonpublic information ↗</a>	CMA_C1084 - Train personnel on disclosure of nonpublic information	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Awareness And Training

### Security Awareness And Training Policy Andprocedures

ID: FedRAMP High AT-1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Document security and privacy training activities ↗</a>	CMA_0198 - Document security and privacy training activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update information security policies ↗</a>	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Awareness Training

ID: FedRAMP High AT-2 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide periodic security awareness training ↗	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 ↗
Provide security training for new users ↗	CMA_0419 - Provide security training for new users	Manual, Disabled	1.1.0 ↗
Provide updated security awareness training ↗	CMA_C1090 - Provide updated security awareness training	Manual, Disabled	1.1.0 ↗

## Insider Threat

ID: FedRAMP High AT-2 (2) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide security awareness training for insider threats ↗	CMA_0417 - Provide security awareness training for insider threats	Manual, Disabled	1.1.0 ↗

## Role-Based Security Training

ID: FedRAMP High AT-3 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide periodic role-based security training ↗	CMA_C1095 - Provide periodic role-based security training	Manual, Disabled	1.1.0 ↗
Provide role-based security training ↗	CMA_C1094 - Provide role-based security training	Manual, Disabled	1.1.0 ↗
Provide security training before providing access ↗	CMA_0418 - Provide security training before providing access	Manual, Disabled	1.1.0 ↗

## Practical Exercises

ID: FedRAMP High AT-3 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide role-based practical exercises ↗	CMA_C1096 - Provide role-based practical exercises	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Suspicious Communications And Anomalous System Behavior

ID: FedRAMP High AT-3 (4) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide role-based training on suspicious activities ↗	CMA_C1097 - Provide role-based training on suspicious activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Training Records

ID: FedRAMP High AT-4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor security and privacy training completion ↗	CMA_0379 - Monitor security and privacy training completion	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Retain training records ↗	CMA_0456 - Retain training records	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Audit And Accountability

### Audit And Accountability Policy And

## Procedures

ID: FedRAMP High AU-1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop audit and accountability policies and procedures ↗	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	1.1.0 ↗
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗

## Audit Events

ID: FedRAMP High AU-2 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↗

## Reviews And Updates

ID: FedRAMP High AU-2 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update the events defined in AU-02 ↗	CMA_C1106 - Review and update the events defined in AU-02	Manual, Disabled	1.1.0 ↗

## Content Of Audit Records

ID: FedRAMP High AU-3 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↗

## Additional Audit Information

ID: FedRAMP High AU-3 (1) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Configure Azure Audit capabilities ↗	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	1.1.1 ↗

## Audit Storage Capacity

ID: FedRAMP High AU-4 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Govern and monitor audit processing activities ↗	CMA_0289 - Govern and monitor audit processing activities	Manual, Disabled	1.1.0 ↗

## Response To Audit Processing Failures

ID: FedRAMP High AU-5 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Govern and monitor audit processing activities ↗	CMA_0289 - Govern and monitor audit processing activities	Manual, Disabled	1.1.0 ↗

## Real-Time Alerts

ID: FedRAMP High AU-5 (2) Ownership: Shared

⋮ Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide real-time alerts for audit event failures ↗	CMA_C1114 - Provide real-time alerts for audit event failures	Manual, Disabled	1.1.0 ↗

## Audit Review, Analysis, And Reporting

ID: FedRAMP High AU-6 Ownership: Shared

⋮ Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .	AuditIfNotExists, Disabled	6.0.0-preview ↗
[Preview]: Network traffic data collection agent should be installed on Linux	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
virtual machines ↗			
[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
Azure Defender for App Service should be enabled ↗	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Azure SQL Database servers should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for DNS should be enabled ↗	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for Key Vault should be enabled ↗	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Resource Manager	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
should be enabled ↗	about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for SQL servers on machines should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	2.0.1 ↗
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↗
Correlate audit records ↗	CMA_0087 - Correlate audit records	Manual, Disabled	1.1.0 ↗
Establish requirements for audit review and reporting ↗	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	1.1.0 ↗
Integrate audit review, ↗	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
analysis, and reporting ↗			
Integrate cloud app security with a siem ↗	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	1.1.0 ↗
Microsoft Defender for Containers should be enabled ↗	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	1.0.0 ↗
Microsoft Defender for Storage should be enabled ↗	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	1.0.0 ↗
Network Watcher should be enabled ↗	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	3.0.0 ↗
Review account provisioning logs ↗	CMA_0460 - Review account provisioning logs	Manual, Disabled	1.1.0 ↗
Review administrator assignments weekly ↗	CMA_0461 - Review administrator assignments weekly	Manual, Disabled	1.1.0 ↗
Review audit data ↗	CMA_0466 - Review audit data	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review cloud identity report overview ↗	CMA_0468 - Review cloud identity report overview	Manual, Disabled	1.1.0 ↗
Review controlled folder access events ↗	CMA_0471 - Review controlled folder access events	Manual, Disabled	1.1.0 ↗
Review file and folder activity ↗	CMA_0473 - Review file and folder activity	Manual, Disabled	1.1.0 ↗
Review role group changes weekly ↗	CMA_0476 - Review role group changes weekly	Manual, Disabled	1.1.0 ↗

## Process Integration

ID: FedRAMP High AU-6 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Correlate audit records ↗	CMA_0087 - Correlate audit records	Manual, Disabled	1.1.0 ↗
Establish requirements for audit review and reporting ↗	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	1.1.0 ↗
Integrate audit review, analysis, and reporting ↗	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	1.1.0 ↗
Integrate cloud app security with a siem ↗	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	1.1.0 ↗
Review account provisioning logs ↗	CMA_0460 - Review account provisioning logs	Manual, Disabled	1.1.0 ↗
Review administrator assignments weekly ↗	CMA_0461 - Review administrator assignments weekly	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review audit data ↗</a>	CMA_0466 - Review audit data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review cloud identity report overview ↗</a>	CMA_0468 - Review cloud identity report overview	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review controlled folder access events ↗</a>	CMA_0471 - Review controlled folder access events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review file and folder activity ↗</a>	CMA_0473 - Review file and folder activity	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review role group changes weekly ↗</a>	CMA_0476 - Review role group changes weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Correlate Audit Repositories

ID: FedRAMP High AU-6 (3) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Correlate audit records ↗</a>	CMA_0087 - Correlate audit records	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Integrate cloud app security with a siem ↗</a>	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Central Review And Analysis

ID: FedRAMP High AU-6 (4) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Preview]: Azure Arc enabled Kubernetes clusters should</a>	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes	AuditIfNotExists, Disabled	<a href="#">6.0.0-preview ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
have Microsoft Defender for Cloud extension installed ↗	backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .		
[Preview]: Log Analytics extension should be installed on your Linux Azure Arc machines ↗	This policy audits Linux Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1-preview ↗
[Preview]: Log Analytics extension should be installed on your Windows Azure Arc machines ↗	This policy audits Windows Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1-preview ↗
[Preview]: Network traffic data collection agent should be installed on Linux virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
App Service apps should have resource logs enabled ↗	Audit enabling of resource logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised.	AuditIfNotExists, Disabled	2.0.1 ↗
Auditing on SQL server	Auditing on your SQL Server should be enabled to track database activities across all databases	AuditIfNotExists, Disabled	2.0.0 ↗

Name should be enabled ↗ (Azure portal)	Description	Effect(s)	Version (GitHub)
Auto provisioning of the Log Analytics agent should be enabled on your subscription ↗	To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.	AuditIfNotExists, Disabled	1.0.1 ↗
Azure Defender for App Service should be enabled ↗	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Azure SQL Database servers should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for DNS should be enabled ↗	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for Key Vault should be enabled ↗	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Resource Manager	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
should be enabled ↗	about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
Azure Defender for SQL servers on machines should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Guest Configuration extension should be installed on your machines ↗	To ensure secure configurations of in-guest settings of your machine, install the Guest Configuration extension. In-guest settings that the extension monitors include the configuration of the operating system, application configuration or presence, and environment settings. Once installed, in-guest policies will be available such as 'Windows Exploit guard should be enabled'. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Log Analytics agent should be installed on your virtual machine for Azure Security Center monitoring ↴	This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring ↴	Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Microsoft Defender for Containers should be enabled ↴	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Microsoft Defender for Storage should be enabled ↴	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Network Watcher should be enabled ↴	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Resource logs in Azure Data Lake Store should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Azure Stream Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Batch accounts should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Data Lake Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Event Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in IoT Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
Resource logs in Key Vault should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Logic Apps should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.1.0 ↗</a>
Resource logs in Search	Audit enabling of resource logs. This enables you to recreate activity trails to use for	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">services should be enabled ↗</a>	investigation purposes; when a security incident occurs or when your network is compromised		
<a href="#">Resource logs in Service Bus should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity ↗</a>	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>

## Integration / Scanning And Monitoring Capabilities

ID: FedRAMP High AU-6 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗</a>	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .	AuditIfNotExists, Disabled	<a href="#">6.0.0-preview ↗</a>
<a href="#">[Preview]: Log Analytics extension should be installed on your Linux</a>	This policy audits Linux Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	<a href="#">1.0.1-preview ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Azure Arc machines ↗</a>			
<a href="#">[Preview]: Log Analytics extension should be installed on your Windows Azure Arc machines ↗</a>	This policy audits Windows Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	<a href="#">1.0.1-preview ↗</a>
<a href="#">[Preview]: Network traffic data collection agent should be installed on Linux virtual machines ↗</a>	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	<a href="#">1.0.2-preview ↗</a>
<a href="#">[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗</a>	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	<a href="#">1.0.2-preview ↗</a>
<a href="#">App Service apps should have resource logs enabled ↗</a>	Audit enabling of resource logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised.	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Auditing on SQL server should be enabled ↗</a>	Auditing on your SQL Server should be enabled to track database activities across all databases on the server and save them in an audit log.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Auto provisioning of the Log Analytics agent should be enabled on your subscription ↗</a>	To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.		
Azure Defender for App Service should be enabled ↗	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Azure SQL Database servers should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for DNS should be enabled ↗	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for Key Vault should be enabled ↗	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Resource Manager should be enabled ↗	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for servers should be enabled ↴	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↴
Azure Defender for SQL servers on machines should be enabled ↴	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↴
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↴	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	2.0.1 ↴
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↴	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↴
Guest Configuration extension should be installed on your machines ↴	To ensure secure configurations of in-guest settings of your machine, install the Guest Configuration extension. In-guest settings that the extension monitors include the configuration of the operating system, application configuration or presence, and environment settings. Once installed, in-guest policies will be available such as 'Windows Exploit guard should be enabled'. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴.	AuditIfNotExists, Disabled	1.0.3 ↴
Integrate Audit record analysis ↴	CMA_C1120 - Integrate Audit record analysis	Manual, Disabled	1.1.0 ↴
Log Analytics agent should be installed on your virtual machine for	This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats	AuditIfNotExists, Disabled	1.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Security Center monitoring ↗			
Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring ↗	Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.	AuditIfNotExists, Disabled	1.0.0 ↗
Microsoft Defender for Containers should be enabled ↗	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	1.0.0 ↗
Microsoft Defender for Storage should be enabled ↗	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	1.0.0 ↗
Network Watcher should be enabled ↗	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	3.0.0 ↗
Resource logs in Azure Data Lake Store should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	5.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Resource logs in Azure Stream Analytics should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Resource logs in Batch accounts should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Resource logs in Data Lake Analytics should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Resource logs in Event Hub should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Resource logs in IoT Hub should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
<a href="#">Resource logs in Key Vault should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Resource logs in Logic Apps should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.1.0 ↗</a>
<a href="#">Resource logs in Search services should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Resource logs in Service Bus</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
should be enabled ↴	investigation purposes; when a security incident occurs or when your network is compromised		
Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity ↴	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴	AuditIfNotExists, Disabled	1.0.1 ↴

## Permitted Actions

ID: FedRAMP High AU-6 (7) Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Specify permitted actions associated with customer audit information ↴	CMA_C1122 - Specify permitted actions associated with customer audit information	Manual, Disabled	1.1.0 ↴

## Audit Level Adjustment

ID: FedRAMP High AU-6 (10) Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Adjust level of audit review, analysis, and reporting ↴	CMA_C1123 - Adjust level of audit review, analysis, and reporting	Manual, Disabled	1.1.0 ↴

## Audit Reduction And Report Generation

ID: FedRAMP High AU-7 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure audit records are not altered ↴	CMA_C1125 - Ensure audit records are not altered	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Provide audit review, analysis, and reporting capability ↴	CMA_C1124 - Provide audit review, analysis, and reporting capability	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Automatic Processing

ID: FedRAMP High AU-7 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide capability to process customer-controlled audit records ↴	CMA_C1126 - Provide capability to process customer-controlled audit records	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Time Stamps

ID: FedRAMP High AU-8 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Use system clocks for audit records ↴	CMA_0535 - Use system clocks for audit records	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Synchronization With Authoritative Time Source

ID: FedRAMP High AU-8 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Use system clocks for audit records ↗	CMA_0535 - Use system clocks for audit records	Manual, Disabled	1.1.0 ↗

## Protection Of Audit Information

ID: FedRAMP High AU-9 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enable dual or joint authorization ↗	CMA_0226 - Enable dual or joint authorization	Manual, Disabled	1.1.0 ↗
Protect audit information ↗	CMA_0401 - Protect audit information	Manual, Disabled	1.1.0 ↗

## Audit Backup On Separate Physical Systems / Components

ID: FedRAMP High AU-9 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish backup policies and procedures ↗	CMA_0268 - Establish backup policies and procedures	Manual, Disabled	1.1.0 ↗

## Cryptographic Protection

ID: FedRAMP High AU-9 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Maintain integrity of audit system ↗	CMA_C1133 - Maintain integrity of audit system	Manual, Disabled	1.1.0 ↗

## Access By Subset Of Privileged Users

ID: FedRAMP High AU-9 (4) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Protect audit information ↗	CMA_0401 - Protect audit information	Manual, Disabled	1.1.0 ↗

## Non-Repudiation

ID: FedRAMP High AU-10 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish electronic signature and certificate requirements ↗	CMA_0271 - Establish electronic signature and certificate requirements	Manual, Disabled	1.1.0 ↗

## Audit Record Retention

ID: FedRAMP High AU-11 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adhere to retention periods defined ↗	CMA_0004 - Adhere to retention periods defined	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Retain security policies and procedures ↗	CMA_0454 - Retain security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
SQL servers with auditing to storage account destination should be configured with 90 days retention or higher ↗	<p>For incident investigation purposes, we recommend setting the data retention for your SQL Server' auditing to storage account destination to at least 90 days.</p> <p>Confirm that you are meeting the necessary retention rules for the regions in which you are operating. This is sometimes required for compliance with regulatory standards.</p>	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Audit Generation

ID: FedRAMP High AU-12 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗	<p>Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a>.</p>	AuditIfNotExists, Disabled	<a href="#">6.0.0-preview ↗</a>
[Preview]: Log Analytics extension should be installed on your Linux Azure Arc machines ↗	This policy audits Linux Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	<a href="#">1.0.1-preview ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Log Analytics extension should be installed on your Windows Azure Arc machines ↗	This policy audits Windows Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1-preview ↗
[Preview]: Network traffic data collection agent should be installed on Linux virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
App Service apps should have resource logs enabled ↗	Audit enabling of resource logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised.	AuditIfNotExists, Disabled	2.0.1 ↗
Audit privileged functions ↗	CMA_0019 - Audit privileged functions	Manual, Disabled	1.1.0 ↗
Audit user account status ↗	CMA_0020 - Audit user account status	Manual, Disabled	1.1.0 ↗
Auditing on SQL server should be enabled ↗	Auditing on your SQL Server should be enabled to track database activities across all databases on the server and save them in an audit log.	AuditIfNotExists, Disabled	2.0.0 ↗
Auto provisioning of the Log Analytics agent should be	To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which	AuditIfNotExists, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">enabled on your subscription ↗</a>	reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.		
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Resource Manager should be enabled ↗</a>	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
Azure Defender for SQL servers on machines should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Guest Configuration extension should be installed on your machines ↗	To ensure secure configurations of in-guest settings of your machine, install the Guest Configuration extension. In-guest settings that the extension monitors include the configuration of the operating system, application configuration or presence, and environment settings. Once installed, in-guest policies will be available such as 'Windows Exploit guard should be enabled'. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Log Analytics agent should be installed on your virtual machine for Azure Security Center monitoring ↗</a>	This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring ↗</a>	Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Containers should be enabled ↗</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Network Watcher should be enabled ↗</a>	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Resource logs in Azure Data Lake Store should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Azure Stream Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Batch accounts should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Data Lake Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Event Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in IoT Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
Resource logs in Key Vault should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Logic Apps should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.1.0 ↗</a>
Resource logs in Search	Audit enabling of resource logs. This enables you to recreate activity trails to use for	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">services should be enabled ↗</a>	investigation purposes; when a security incident occurs or when your network is compromised		
<a href="#">Resource logs in Service Bus should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Review audit data ↗</a>	CMA_0466 - Review audit data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity ↗</a>	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>

## System-Wide / Time-Correlated Audit Trail

ID: FedRAMP High AU-12 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗</a>	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .	AuditIfNotExists, Disabled	<a href="#">6.0.0-preview ↗</a>
<a href="#">[Preview]: Log Analytics extension</a>	This policy audits Linux Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	<a href="#">1.0.1-preview ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
should be installed on your Linux Azure Arc machines ↗			
[Preview]: Log Analytics extension should be installed on your Windows Azure Arc machines ↗	This policy audits Windows Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1-preview ↗
[Preview]: Network traffic data collection agent should be installed on Linux virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
App Service apps should have resource logs enabled ↗	Audit enabling of resource logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised.	AuditIfNotExists, Disabled	2.0.1 ↗
Auditing on SQL server should be enabled ↗	Auditing on your SQL Server should be enabled to track database activities across all databases on the server and save them in an audit log.	AuditIfNotExists, Disabled	2.0.0 ↗
Auto provisioning of the Log Analytics agent should be enabled on	To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations	AuditIfNotExists, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">your subscription ↗</a>	and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.		
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Resource Manager should be enabled ↗</a>	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for servers should be enabled ↴	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>
Azure Defender for SQL servers on machines should be enabled ↴	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↴	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↴</a>
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↴	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>
Compile Audit records into system wide audit ↴	CMA_C1140 - Compile Audit records into system wide audit	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Guest Configuration extension should be installed on your machines ↴	To ensure secure configurations of in-guest settings of your machine, install the Guest Configuration extension. In-guest settings that the extension monitors include the configuration of the operating system, application configuration or presence, and environment settings. Once installed, in-guest policies will be available such as 'Windows Exploit guard should be enabled'. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Log Analytics agent should be installed on your virtual machine for Azure Security Center monitoring ↗</a>	This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring ↗</a>	Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Containers should be enabled ↗</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Network Watcher should be enabled ↗</a>	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Resource logs in Azure Data Lake Store should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Azure Stream Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Batch accounts should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Data Lake Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Event Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in IoT Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
Resource logs in Key Vault should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Logic Apps should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.1.0 ↗</a>
Resource logs in Search	Audit enabling of resource logs. This enables you to recreate activity trails to use for	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">services should be enabled ↴</a>	investigation purposes; when a security incident occurs or when your network is compromised		
<a href="#">Resource logs in Service Bus should be enabled ↴</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↴</a>
<a href="#">Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity ↴</a>	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↴</a>

## Changes By Authorized Individuals

ID: FedRAMP High AU-12 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Provide the capability to extend or limit auditing on customer-deployed resources ↴</a>	CMA_C1141 - Provide the capability to extend or limit auditing on customer-deployed resources	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Security Assessment And Authorization

### Security Assessment And Authorization

Policy And Procedures

ID: FedRAMP High CA-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review security assessment and authorization policies and procedures ↗	CMA_C1143 - Review security assessment and authorization policies and procedures	Manual, Disabled	1.1.0 ↗

## Security Assessments

ID: FedRAMP High CA-2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess Security Controls ↗	CMA_C1145 - Assess Security Controls	Manual, Disabled	1.1.0 ↗
Deliver security assessment results ↗	CMA_C1147 - Deliver security assessment results	Manual, Disabled	1.1.0 ↗
Develop security assessment plan ↗	CMA_C1144 - Develop security assessment plan	Manual, Disabled	1.1.0 ↗
Produce Security Assessment report ↗	CMA_C1146 - Produce Security Assessment report	Manual, Disabled	1.1.0 ↗

## Independent Assessors

ID: FedRAMP High CA-2 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ independent assessors to conduct security control assessments ↗	CMA_C1148 - Employ independent assessors to conduct security control assessments	Manual, Disabled	1.1.0 ↗

## Specialized Assessments

ID: FedRAMP High CA-2 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Select additional testing for security control assessments ↗	CMA_C1149 - Select additional testing for security control assessments	Manual, Disabled	1.1.0 ↗

## External Organizations

ID: FedRAMP High CA-2 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Accept assessment results ↗	CMA_C1150 - Accept assessment results	Manual, Disabled	1.1.0 ↗

## System Interconnections

ID: FedRAMP High CA-3 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require interconnection security agreements ↗	CMA_C1151 - Require interconnection security agreements	Manual, Disabled	1.1.0 ↗
Update interconnection security agreements ↗	CMA_0519 - Update interconnection security agreements	Manual, Disabled	1.1.0 ↗

## Unclassified Non-National Security System Connections

ID: FedRAMP High CA-3 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Restrictions On External System Connections

ID: FedRAMP High CA-3 (5) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ restrictions on external system interconnections ↗	CMA_C1155 - Employ restrictions on external system interconnections	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Plan Of Action And Milestones

ID: FedRAMP High CA-5 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop POA&M ↗	CMA_C1156 - Develop POA&M	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update POA&M items ↗	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Authorization

ID: FedRAMP High CA-6 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign an authorizing official (AO) ↗	CMA_C1158 - Assign an authorizing official (AO)	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Ensure resources are	CMA_C1159 - Ensure resources are	Manual,	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">authorized ↗</a>	authorized	Disabled	
<a href="#">Update the security authorization ↗</a>	CMA_C1160 - Update the security authorization	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Continuous Monitoring

ID: FedRAMP High CA-7 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Configure detection whitelist ↗</a>	CMA_0068 - Configure detection whitelist	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Turn on sensors for endpoint security solution ↗</a>	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Undergo independent security review ↗</a>	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Independent Assessment

ID: FedRAMP High CA-7 (1) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ independent assessors for continuous monitoring ↗</a>	CMA_C1168 - Employ independent assessors for continuous monitoring	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Trend Analyses

ID: FedRAMP High CA-7 (3) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Analyse data obtained from continuous monitoring ↗	CMA_C1169 - Analyse data obtained from continuous monitoring	Manual, Disabled	1.1.0 ↗

## Independent Penetration Agent Or Team

ID: FedRAMP High CA-8 (1) Ownership: Shared

[] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ independent team for penetration testing ↗	CMA_C1171 - Employ independent team for penetration testing	Manual, Disabled	1.1.0 ↗

## Internal System Connections

ID: FedRAMP High CA-9 Ownership: Shared

[] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Check for privacy and security compliance before establishing internal connections ↗	CMA_0053 - Check for privacy and security compliance before establishing internal connections	Manual, Disabled	1.1.0 ↗

## Configuration Management

### Configuration Management Policy And Procedures

ID: FedRAMP High CM-1 Ownership: Shared

[] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update configuration management policies and procedures ↗	CMA_C1175 - Review and update configuration management policies and procedures	Manual, Disabled	1.1.0 ↗

## Baseline Configuration

ID: FedRAMP High CM-2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure actions for noncompliant devices ↗	CMA_0062 - Configure actions for noncompliant devices	Manual, Disabled	1.1.0 ↗
Develop and maintain baseline configurations ↗	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	1.1.0 ↗
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗
Establish a configuration control board ↗	CMA_0254 - Establish a configuration control board	Manual, Disabled	1.1.0 ↗
Establish and document a configuration management plan ↗	CMA_0264 - Establish and document a configuration management plan	Manual, Disabled	1.1.0 ↗
Implement an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	1.1.0 ↗

## Automation Support For Accuracy / Currency

ID: FedRAMP High CM-2 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure actions for	CMA_0062 - Configure actions for	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">noncompliant devices ↗</a>	noncompliant devices	Disabled	
<a href="#">Develop and maintain baseline configurations ↗</a>	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce security configuration settings ↗</a>	CMA_0249 - Enforce security configuration settings	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a configuration control board ↗</a>	CMA_0254 - Establish a configuration control board	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and document a configuration management plan ↗</a>	CMA_0264 - Establish and document a configuration management plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement an automated configuration management tool ↗</a>	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Retention Of Previous Configurations

ID: FedRAMP High CM-2 (3) Ownership: Shared

[\[ \] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Retain previous versions of baseline configs ↗</a>	CMA_C1181 - Retain previous versions of baseline configs	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Configure Systems, Components, Or Devices For High-Risk Areas

ID: FedRAMP High CM-2 (7) Ownership: Shared

[\[ \] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Ensure security safeguards not needed when the individuals</a>	CMA_C1183 - Ensure security safeguards not needed when the	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">return ↗</a>	individuals return		
<a href="#">Not allow for information systems to accompany with individuals ↗</a>	CMA_C1182 - Not allow for information systems to accompany with individuals	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Configuration Change Control

ID: FedRAMP High CM-3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Conduct a security impact analysis ↗</a>	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop and maintain a vulnerability management standard ↗</a>	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a risk management strategy ↗</a>	CMA_0258 - Establish a risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and document change control processes ↗</a>	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish configuration management requirements for developers ↗</a>	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a privacy impact assessment ↗</a>	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a risk assessment ↗</a>	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform audit for configuration change control ↗</a>	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Document / Notification / Prohibition Of Changes

ID: FedRAMP High CM-3 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Automate approval request for proposed changes ↗</a>	CMA_C1192 - Automate approval request for proposed changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate implementation of approved change notifications ↗</a>	CMA_C1196 - Automate implementation of approved change notifications	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate process to document implemented changes ↗</a>	CMA_C1195 - Automate process to document implemented changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate process to highlight unreviewed change proposals ↗</a>	CMA_C1193 - Automate process to highlight unreviewed change proposals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate process to prohibit implementation of unapproved changes ↗</a>	CMA_C1194 - Automate process to prohibit implementation of unapproved changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate proposed documented changes ↗</a>	CMA_C1191 - Automate proposed documented changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Test / Validate / Document Changes

ID: FedRAMP High CM-3 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish and document change control processes ↗</a>	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish configuration management requirements for developers ↗</a>	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform audit for configuration change control ↗</a>	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Representative

ID: FedRAMP High CM-3 (4) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign information security representative to change control ↗	CMA_C1198 - Assign information security representative to change control	Manual, Disabled	1.1.0 ↗

## Cryptography Management

ID: FedRAMP High CM-3 (6) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure cryptographic mechanisms are under configuration management ↗	CMA_C1199 - Ensure cryptographic mechanisms are under configuration management	Manual, Disabled	1.1.0 ↗

## Security Impact Analysis

ID: FedRAMP High CM-4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Develop and maintain a vulnerability management standard ↗	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	1.1.0 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for	CMA_0270 - Establish configuration management requirements for	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
developers ↗	developers		
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	1.1.0 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	1.1.0 ↗
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗

## Separate Test Environments

ID: FedRAMP High CM-4 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	1.1.0 ↗
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗

## Access Restrictions For Change

ID: FedRAMP High CM-5 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗

## Automated Access Enforcement / Auditing

ID: FedRAMP High CM-5 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce and audit access restrictions ↗	CMA_C1203 - Enforce and audit access restrictions	Manual, Disabled	1.1.0 ↗

## Review System Changes

ID: FedRAMP High CM-5 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review changes for any unauthorized changes ↗	CMA_C1204 - Review changes for any unauthorized changes	Manual, Disabled	1.1.0 ↗

## Signed Components

ID: FedRAMP High CM-5 (3) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Restrict unauthorized software and firmware installation ↗	CMA_C1205 - Restrict unauthorized software and firmware installation	Manual, Disabled	1.1.0 ↗

## Limit Production / Operational Privileges

ID: FedRAMP High CM-5 (5) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Limit privileges to make changes in production environment ↗</a>	CMA_C1206 - Limit privileges to make changes in production environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and reevaluate privileges ↗</a>	CMA_C1207 - Review and reevaluate privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Configuration Settings

ID: FedRAMP High CM-6 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Deprecated]: Function apps should have 'Client Certificates (Incoming client certificates)' enabled ↗</a>	Client certificates allow for the app to request a certificate for incoming requests. Only clients with valid certificates will be able to reach the app. This policy has been replaced by a new policy with the same name because Http 2.0 doesn't support client certificates.	Audit, Disabled	<a href="#">3.1.0-deprecated ↗</a>
<a href="#">App Service apps should have Client Certificates (Incoming client certificates) enabled ↗</a>	Client certificates allow for the app to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the app. This policy applies to apps with Http version set to 1.1.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">App Service apps should have remote debugging turned off ↗</a>	Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">App Service apps should not</a>	Cross-Origin Resource Sharing (CORS) should not allow all domains to access	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">have CORS configured to allow every resource to access your apps ↗</a>	your app. Allow only required domains to interact with your app.		
<a href="#">Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your clusters ↗</a>	Azure Policy Add-on for Kubernetes service (AKS) extends Gatekeeper v3, an admission controller webhook for Open Policy Agent (OPA), to apply at-scale enforcements and safeguards on your clusters in a centralized, consistent manner.	Audit, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Enforce security configuration settings ↗</a>	CMA_0249 - Enforce security configuration settings	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Function apps should have remote debugging turned off ↗</a>	Remote debugging requires inbound ports to be opened on Function apps. Remote debugging should be turned off.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Function apps should not have CORS configured to allow every resource to access your apps ↗</a>	Cross-Origin Resource Sharing (CORS) should not allow all domains to access your Function app. Allow only required domains to interact with your Function app.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Kubernetes cluster containers CPU and memory resource limits should not exceed the specified limits ↗</a>	Enforce container CPU and memory resource limits to prevent resource exhaustion attacks in a Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">9.1.0 ↗</a>
<a href="#">Kubernetes cluster containers should not</a>	Block pod containers from sharing the host process ID namespace and host IPC namespace in a Kubernetes cluster. This recommendation is part of CIS 5.2.2 and	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">5.1.0 ↗</a>

Name	Description	Effect(s)	Version
			(GitHub)
share host process ID or (Azure portal) host IPC namespace ↴	CIS 5.2.3 which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .		
Kubernetes cluster containers should only use allowed AppArmor profiles ↴	Containers should only use allowed AppArmor profiles in a Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.1 ↴
Kubernetes cluster containers should only use allowed capabilities ↴	Restrict the capabilities to reduce the attack surface of containers in a Kubernetes cluster. This recommendation is part of CIS 5.2.8 and CIS 5.2.9 which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.0 ↴
Kubernetes cluster containers should only use allowed images ↴	Use images from trusted registries to reduce the Kubernetes cluster's exposure risk to unknown vulnerabilities, security issues and malicious images. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	9.1.1 ↴
Kubernetes cluster containers should run with a read only root file system ↴	Run containers with a read only root file system to protect from changes at runtime with malicious binaries being added to PATH in a Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.0 ↴
Kubernetes cluster pod hostPath volumes should only use allowed host paths ↴	Limit pod HostPath volume mounts to the allowed host paths in a Kubernetes Cluster. This policy is generally available for Kubernetes Service (AKS), and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.1 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Kubernetes cluster pods and containers should only run with approved user and group IDs</a>	Control the user, primary group, supplemental group and file system group IDs that pods and containers can use to run in a Kubernetes Cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.1
<a href="#">Kubernetes cluster pods should only use approved host network and port range</a>	Restrict pod access to the host network and the allowable host port range in a Kubernetes cluster. This recommendation is part of CIS 5.2.4 which is intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.0
<a href="#">Kubernetes cluster services should listen only on allowed ports</a>	Restrict services to listen only on allowed ports to secure access to the Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	8.1.0
<a href="#">Kubernetes cluster should not allow privileged containers</a>	Do not allow privileged containers creation in a Kubernetes cluster. This recommendation is part of CIS 5.2.1 which is intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	9.1.0
<a href="#">Kubernetes clusters should not allow container privilege escalation</a>	Do not allow containers to run with privilege escalation to root in a Kubernetes cluster. This recommendation is part of CIS 5.2.5 which is intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more	audit, Audit, deny, Deny, disabled, Disabled	7.1.0

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .		
Linux machines should meet requirements for the Azure compute security baseline ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if the machine is not configured correctly for one of the recommendations in the Azure compute security baseline.	AuditIfNotExists, Disabled	2.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗
Windows machines should meet requirements of the Azure compute security baseline ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if the machine is not configured correctly for one of the recommendations in the Azure compute security baseline.	AuditIfNotExists, Disabled	2.0.0 ↗

## Automated Central Management / Application / Verification

ID: FedRAMP High CM-6 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗
Govern compliance of cloud service providers ↗	CMA_0290 - Govern compliance of cloud service providers	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

## Least Functionality

ID: FedRAMP High CM-7 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications should be enabled on your machines ↗</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Azure Defender for servers should be enabled ↗</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

## Prevent Program Execution

ID: FedRAMP High CM-7 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should be enabled on your machines ↗</a>	rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.		
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Authorized Software / Whitelisting

ID: FedRAMP High CM-7 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications should be enabled on your machines ↗</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

# Information System Component Inventory

ID: FedRAMP High CM-8 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Create a data inventory ↗</a>	CMA_0096 - Create a data inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Maintain records of processing of personal data ↗</a>	CMA_0353 - Maintain records of processing of personal data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Updates During Installations / Removals

ID: FedRAMP High CM-8 (1) Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Create a data inventory ↗</a>	CMA_0096 - Create a data inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Maintain records of processing of personal data ↗</a>	CMA_0353 - Maintain records of processing of personal data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Unauthorized Component Detection

ID: FedRAMP High CM-8 (3) Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Enable detection of network devices ↗</a>	CMA_0220 - Enable detection of network devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Set automated notifications for new and trending cloud applications in your organization ↗</a>	CMA_0495 - Set automated notifications for new and trending cloud applications in your organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Accountability Information

ID: FedRAMP High CM-8 (4) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Create a data inventory ↗</a>	CMA_0096 - Create a data inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and maintain an asset inventory ↗</a>	CMA_0266 - Establish and maintain an asset inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Configuration Management Plan

ID: FedRAMP High CM-9 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Create configuration plan protection ↗</a>	CMA_C1233 - Create configuration plan protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop and maintain baseline configurations ↗</a>	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop configuration item identification plan ↗</a>	CMA_C1231 - Develop configuration item identification plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop configuration management plan ↗</a>	CMA_C1232 - Develop configuration management plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and document a configuration management plan ↗</a>	CMA_0264 - Establish and document a configuration management plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement an automated configuration management tool ↗</a>	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Software Usage Restrictions

ID: FedRAMP High CM-10 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications should be enabled on your machines ↗</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Require compliance with intellectual property rights ↗</a>	CMA_0432 - Require compliance with intellectual property rights	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Track software license usage ↗</a>	CMA_C1235 - Track software license usage	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Open Source Software

ID: FedRAMP High CM-10 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Restrict use of open source software ↗</a>	CMA_C1237 - Restrict use of open source software	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## User-Installed Software

ID: FedRAMP High CM-11 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications should be enabled on your machines ↗</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Contingency Planning

### Contingency Planning Policy And Procedures

ID: FedRAMP High CP-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update contingency planning policies and procedures ↗</a>	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Contingency Plan

ID: FedRAMP High CP-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Communicate contingency plan changes ↗	CMA_C1249 - Communicate contingency plan changes	Manual, Disabled	1.1.0 ↗
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	1.1.0 ↗
Develop and document a business continuity and disaster recovery plan ↗	CMA_0146 - Develop and document a business continuity and disaster recovery plan	Manual, Disabled	1.1.0 ↗
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0 ↗
Develop contingency planning policies and procedures ↗	CMA_0156 - Develop contingency planning policies and procedures	Manual, Disabled	1.1.0 ↗
Distribute policies and procedures ↗	CMA_0185 - Distribute policies and procedures	Manual, Disabled	1.1.0 ↗
Review contingency plan ↗	CMA_C1247 - Review contingency plan	Manual, Disabled	1.1.0 ↗
Update contingency plan ↗	CMA_C1248 - Update contingency plan	Manual, Disabled	1.1.0 ↗

## Coordinate With Related Plans

ID: FedRAMP High CP-2 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	1.1.0 ↗

## Capacity Planning

ID: FedRAMP High CP-2 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct capacity planning ↗	CMA_C1252 - Conduct capacity planning	Manual, Disabled	1.1.0 ↗

## Resume Essential Missions / Business Functions

ID: FedRAMP High CP-2 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Plan for resumption of essential business functions ↗	CMA_C1253 - Plan for resumption of essential business functions	Manual, Disabled	1.1.0 ↗

## Resume All Missions / Business Functions

ID: FedRAMP High CP-2 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Resume all mission and business functions ↗	CMA_C1254 - Resume all mission and business functions	Manual, Disabled	1.1.0 ↗

## Continue Essential Missions / Business Functions

ID: FedRAMP High CP-2 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Plan for continuance of essential business functions ↗	CMA_C1255 - Plan for continuance of essential business functions	Manual, Disabled	1.1.0 ↗

## Identify Critical Assets

ID: FedRAMP High CP-2 (8) Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Perform a business impact assessment and application criticality assessment ↗</a>	CMA_0386 - Perform a business impact assessment and application criticality assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Contingency Training

ID: FedRAMP High CP-3 Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Provide contingency training ↗</a>	CMA_0412 - Provide contingency training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Simulated Events

ID: FedRAMP High CP-3 (1) Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Incorporate simulated contingency training ↗</a>	CMA_C1260 - Incorporate simulated contingency training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Contingency Plan Testing

ID: FedRAMP High CP-4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Initiate contingency plan testing corrective actions ↗</a>	CMA_C1263 - Initiate contingency plan testing corrective actions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review the results of contingency plan testing ↗</a>	CMA_C1262 - Review the results of contingency plan testing	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Test the business continuity and disaster recovery plan ↗</a>	CMA_0509 - Test the business continuity and disaster recovery plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Coordinate With Related Plans

ID: FedRAMP High CP-4 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Coordinate contingency plans with related plans ↗</a>	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Alternate Processing Site

ID: FedRAMP High CP-4 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Evaluate alternate processing site capabilities ↗</a>	CMA_C1266 - Evaluate alternate processing site capabilities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Test contingency plan at an alternate processing location ↗</a>	CMA_C1265 - Test contingency plan at an alternate processing location	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Alternate Storage Site

ID: FedRAMP High CP-6 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Ensure alternate storage site safeguards are equivalent to primary site ↗</a>	CMA_C1268 - Ensure alternate storage site safeguards are equivalent to primary site	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish alternate storage site to store and retrieve backup information ↗</a>	CMA_C1267 - Establish alternate storage site to store and retrieve backup information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Geo-redundant backup should be enabled for Azure Database for MariaDB ↗</a>	Azure Database for MariaDB allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Geo-redundant backup should be enabled for Azure Database for MySQL ↗</a>	Azure Database for MySQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Geo-redundant backup should be enabled for Azure Database for PostgreSQL ↗</a>	Azure Database for PostgreSQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Geo-redundant storage should be used to create highly available applications ↗</a>	Use geo-redundancy to create highly available applications	Audit, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">enabled for Storage Accounts ↗</a>			
<a href="#">Long-term geo-redundant backup should be enabled for Azure SQL Databases ↗</a>	This policy audits any Azure SQL Database with long-term geo-redundant backup not enabled.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

## Separation From Primary Site

ID: FedRAMP High CP-6 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Create separate alternate and primary storage sites ↗</a>	CMA_C1269 - Create separate alternate and primary storage sites	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Geo-redundant backup should be enabled for Azure Database for MariaDB ↗</a>	Azure Database for MariaDB allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Geo-redundant backup should be enabled for Azure Database for MySQL ↗</a>	Azure Database for MySQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Geo-redundant backup should be enabled for Azure Database for PostgreSQL ↗</a>	Azure Database for PostgreSQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Geo-redundant storage should be enabled for Storage Accounts ↗</a>	Use geo-redundancy to create highly available applications	Audit, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Long-term geo-redundant backup should be enabled for Azure SQL Databases ↗</a>	This policy audits any Azure SQL Database with long-term geo-redundant backup not enabled.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

## Recovery Time / Point Objectives

ID: FedRAMP High CP-6 (2) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish alternate storage site that facilitates recovery operations ↗</a>	CMA_C1270 - Establish alternate storage site that facilitates recovery operations	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Accessibility

ID: FedRAMP High CP-6 (3) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Identify and mitigate potential issues at alternate storage site ↗</a>	CMA_C1271 - Identify and mitigate potential issues at alternate storage site	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Alternate Processing Site

ID: FedRAMP High CP-7 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit virtual machines without disaster recovery configured ↗</a>	Audit virtual machines which do not have disaster recovery configured. To learn more about disaster recovery, visit <a href="https://aka.ms/asr-doc">https://aka.ms/asr-doc</a> ↗.	auditIfNotExists	<a href="#">1.0.0 ↗</a>
<a href="#">Establish an alternate processing site ↗</a>	CMA_0262 - Establish an alternate processing site	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Separation From Primary Site

ID: FedRAMP High CP-7 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish an alternate processing site ↗</a>	CMA_0262 - Establish an alternate processing site	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Accessibility

ID: FedRAMP High CP-7 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗

## Priority Of Service

ID: FedRAMP High CP-7 (3) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗
Establish requirements for internet service providers ↗	CMA_0278 - Establish requirements for internet service providers	Manual, Disabled	1.1.0 ↗

## Preparation For Use

ID: FedRAMP High CP-7 (4) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Prepare alternate processing site for use as operational site ↗	CMA_C1278 - Prepare alternate processing site for use as operational site	Manual, Disabled	1.1.0 ↗

## Priority Of Service Provisions

ID: FedRAMP High CP-8 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish requirements for internet service providers ↴	CMA_0278 - Establish requirements for internet service providers	Manual, Disabled	1.1.0 ↴

## Information System Backup

ID: FedRAMP High CP-9 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Backup should be enabled for Virtual Machines ↴	Ensure protection of your Azure Virtual Machines by enabling Azure Backup. Azure Backup is a secure and cost effective data protection solution for Azure.	AuditIfNotExists, Disabled	3.0.0 ↴
Conduct backup of information system documentation ↴	CMA_C1289 - Conduct backup of information system documentation	Manual, Disabled	1.1.0 ↴
Establish backup policies and procedures ↴	CMA_0268 - Establish backup policies and procedures	Manual, Disabled	1.1.0 ↴
Geo-redundant backup should be enabled for Azure Database for MariaDB ↴	Azure Database for MariaDB allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	1.0.1 ↴
Geo-redundant backup should be enabled for Azure Database for MySQL ↴	Azure Database for MySQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure.	Audit, Disabled	1.0.1 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Configuring geo-redundant storage for backup is only allowed during server create.		
<a href="#">Geo-redundant backup should be enabled for Azure Database for PostgreSQL ↗</a>	Azure Database for PostgreSQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Key vaults should have deletion protection enabled ↗</a>	Malicious deletion of a key vault can lead to permanent data loss. You can prevent permanent data loss by enabling purge protection and soft delete. Purge protection protects you from insider attacks by enforcing a mandatory retention period for soft deleted key vaults. No one inside your organization or Microsoft will be able to purge your key vaults during the soft delete retention period. Keep in mind that key vaults created after September 1st 2019 have soft-delete enabled by default.	Audit, Deny, Disabled	<a href="#">2.1.0 ↗</a>
<a href="#">Key vaults should have soft delete enabled ↗</a>	Deleting a key vault without soft delete enabled permanently deletes all secrets, keys, and certificates stored in the key vault. Accidental deletion of a key vault can lead to permanent data loss. Soft delete allows you to recover an accidentally deleted key vault for a configurable retention period.	Audit, Deny, Disabled	<a href="#">3.0.0 ↗</a>

## Separate Storage For Critical Information

ID: FedRAMP High CP-9 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Separately store backup information ↗	CMA_C1293 - Separately store backup information	Manual, Disabled	1.1.0 ↗

## Transfer To Alternate Storage Site

ID: FedRAMP High CP-9 (5) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Transfer backup information to an alternate storage site ↗	CMA_C1294 - Transfer backup information to an alternate storage site	Manual, Disabled	1.1.0 ↗

## Information System Recovery And Reconstitution

ID: FedRAMP High CP-10 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Recover and reconstitute resources after any disruption ↗	CMA_C1295 - Recover and reconstitute resources after any disruption	Manual, Disabled	1.1.1 ↗

## Transaction Recovery

ID: FedRAMP High CP-10 (2) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement transaction based recovery ↗	CMA_C1296 - Implement transaction based recovery	Manual, Disabled	1.1.0 ↗

## Restore Within Time Period

ID: FedRAMP High CP-10 (4) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Restore resources to operational state ↗</a>	CMA_C1297 - Restore resources to operational state	Manual, Disabled	<a href="#">1.1.1 ↗</a>

## Identification And Authentication

### Identification And Authentication Policy And Procedures

ID: FedRAMP High IA-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update identification and authentication policies and procedures ↗</a>	CMA_C1299 - Review and update identification and authentication policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Identification And Authentication

(Organizational Users)

ID: FedRAMP High IA-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accounts with owner permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Accounts with read permissions on Azure resources should be MFA enabled ↗	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	1.0.0 ↗
Accounts with write permissions on Azure resources should be MFA enabled ↗	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	1.0.0 ↗
An Azure Active Directory administrator should be provisioned for SQL servers ↗	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	1.0.0 ↗
App Service apps should use managed identity ↗	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	3.0.0 ↗
Cognitive Services accounts should have local authentication methods disabled ↗	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
Enforce user uniqueness ↗	CMA_0250 - Enforce user uniqueness	Manual, Disabled	1.1.0 ↗
Function apps should use managed identity ↗	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	3.0.0 ↗
Service Fabric clusters should only use Azure Active Directory for client authentication ↗	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	1.1.0 ↗
Support personal verification credentials issued by legal authorities ↗	CMA_0507 - Support personal verification credentials issued by legal authorities	Manual, Disabled	1.1.0 ↗

## Network Access To Privileged Accounts

ID: FedRAMP High IA-2 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accounts with owner permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Accounts with write permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Network Access To Non-Privileged Accounts

ID: FedRAMP High IA-2 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accounts with read permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Local Access To Privileged Accounts

ID: FedRAMP High IA-2 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Group Authentication

ID: FedRAMP High IA-2 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Require use of individual authenticators ↗</a>	CMA_C1305 - Require use of individual authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Remote Access - Separate Device

ID: FedRAMP High IA-2 (11) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify and authenticate network devices ↗</a>	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Acceptance Of Piv Credentials

ID: FedRAMP High IA-2 (12) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Support personal verification credentials issued by legal authorities ↗	CMA_0507 - Support personal verification credentials issued by legal authorities	Manual, Disabled	1.1.0 ↗

## Identifier Management

ID: FedRAMP High IA-4 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An Azure Active Directory administrator should be provisioned for SQL servers ↗	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	1.0.0 ↗
App Service apps should use managed identity ↗	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	3.0.0 ↗
Assign system identifiers ↗	CMA_0018 - Assign system identifiers	Manual, Disabled	1.1.0 ↗
Cognitive Services accounts should have local authentication methods disabled ↗	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> .	Audit, Deny, Disabled	1.0.0 ↗
Function apps should use managed identity ↗	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	3.0.0 ↗
Prevent identifier reuse for the defined time period ↗	CMA_C1314 - Prevent identifier reuse for the defined time period	Manual, Disabled	1.1.0 ↗
Service Fabric clusters should only use Azure Active	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Directory for client authentication ↗			

## Identify User Status

ID: FedRAMP High IA-4 (4) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Identify status of individual users ↗	CMA_C1316 - Identify status of individual users	Manual, Disabled	1.1.0 ↗

## Authenticator Management

ID: FedRAMP High IA-5 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
[Preview]: Certificates should have the specified maximum validity period ↗	Manage your organizational compliance requirements by specifying the maximum amount of time that a certificate can be valid within your key vault.	audit, Audit, deny, Deny, disabled, Disabled	2.2.0-preview ↗
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	modify	4.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	4.0.0 ↗
Audit Linux machines that do not have the passwd file permissions set to 0644 ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Linux machines that do not have the passwd file permissions set to 0644	AuditIfNotExists, Disabled	3.0.0 ↗
Audit Windows machines that do not store passwords using reversible encryption ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not store passwords using reversible encryption	AuditIfNotExists, Disabled	2.0.0 ↗
Authentication to Linux machines should require SSH keys ↗	Although SSH itself provides an encrypted connection, using passwords with SSH still leaves the VM vulnerable to brute-force attacks. The most secure option for authenticating to an Azure Linux virtual machine over SSH is with a public-private key pair, also known as SSH keys. Learn more: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed">https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed</a> .	AuditIfNotExists, Disabled	3.1.0 ↗
Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↗	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more	deployIfNotExists	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .		
<a href="#">Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs</a>	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	<a href="#">1.2.0</a>
<a href="#">Establish authenticator types and processes</a>	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	<a href="#">1.1.0</a>
<a href="#">Establish procedures for initial authenticator distribution</a>	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	<a href="#">1.1.0</a>
<a href="#">Implement training for protecting authenticators</a>	CMA_0329 - Implement training for protecting authenticators	Manual, Disabled	<a href="#">1.1.0</a>
<a href="#">Key Vault keys should have an expiration date</a>	Cryptographic keys should have a defined expiration date and not be permanent. Keys that are valid forever provide a potential attacker with more time to compromise the key. It is a recommended security practice to set expiration dates on cryptographic keys.	Audit, Deny, Disabled	<a href="#">1.0.2</a>
<a href="#">Key Vault secrets should have an expiration date</a>	Secrets should have a defined expiration date and not be permanent. Secrets that are valid forever provide a potential attacker with more time to compromise them. It is a recommended security practice to set expiration dates on secrets.	Audit, Deny, Disabled	<a href="#">1.0.2</a>
<a href="#">Manage authenticator lifetime and reuse</a>	CMA_0355 - Manage authenticator lifetime and reuse	Manual, Disabled	<a href="#">1.1.0</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Manage Authenticators ↴	CMA_C1321 - Manage Authenticators	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Refresh authenticators ↴	CMA_0425 - Refresh authenticators	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Reissue authenticators for changed groups and accounts ↴	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Verify identity before distributing authenticators ↴	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Password-Based Authentication

ID: FedRAMP High IA-5 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↴	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	<a href="#">4.0.0 ↴</a>
Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↴	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy	modify	<a href="#">4.0.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .		
Audit Linux machines that do not have the passwd file permissions set to 0644	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Linux machines that do not have the passwd file permissions set to 0644	AuditIfNotExists, Disabled	3.0.0
Audit Windows machines that allow re-use of the passwords after the specified number of unique passwords	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that allow re-use of the passwords after the specified number of unique passwords. Default value for unique passwords is 24	AuditIfNotExists, Disabled	2.1.0
Audit Windows machines that do not have the maximum password age set to specified number of days	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not have the maximum password age set to specified number of days. Default value for maximum password age is 70 days	AuditIfNotExists, Disabled	2.1.0
Audit Windows machines that do not have the minimum password age set to specified number of days	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not have the minimum password age set to specified number of days. Default value for minimum password age is 1 day	AuditIfNotExists, Disabled	2.1.0
Audit Windows machines that do not have the password complexity setting enabled	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not have the password complexity setting enabled	AuditIfNotExists, Disabled	2.0.0
Audit Windows machines that do not restrict the minimum password length to specified	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not restrict the minimum password length to specified number of characters. Default value	AuditIfNotExists, Disabled	2.1.0

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
number of characters ↗	for minimum password length is 14 characters		
Audit Windows machines that do not store passwords using reversible encryption ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not store passwords using reversible encryption	AuditIfNotExists, Disabled	2.0.0 ↗
Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↗	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	3.0.0 ↗
Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs ↗	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	1.2.0 ↗
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Establish a password policy ↗	CMA_0256 - Establish a password policy	Manual, Disabled	1.1.0 ↗
Implement parameters for memorized secret verifiers ↗	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Pki-Based Authentication

ID: FedRAMP High IA-5 (2) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Bind authenticators and identities dynamically ↗	CMA_0035 - Bind authenticators and identities dynamically	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish authenticator types and processes ↗	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish parameters for searching secret authenticators and verifiers ↗	CMA_0274 - Establish parameters for searching secret authenticators and verifiers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish procedures for initial authenticator distribution ↗	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Map authenticated identities to individuals ↗	CMA_0372 - Map authenticated identities to individuals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Restrict access to private keys ↗	CMA_0445 - Restrict access to private keys	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## In-Person Or Trusted Third-Party Registration

ID: FedRAMP High IA-5 (3) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Distribute authenticators ↗	CMA_0184 - Distribute authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Automated Support For Password Strength Determination

ID: FedRAMP High IA-5 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Document security strength requirements in acquisition contracts ↗</a>	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a password policy ↗</a>	CMA_0256 - Establish a password policy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement parameters for memorized secret verifiers ↗</a>	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Protection Of Authenticators

ID: FedRAMP High IA-5 (6) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Ensure authorized users protect provided authenticators ↗</a>	CMA_C1339 - Ensure authorized users protect provided authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# No Embedded Unencrypted Static Authenticators

ID: FedRAMP High IA-5 (7) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Ensure there are no unencrypted static authenticators ↗</a>	CMA_C1340 - Ensure there are no unencrypted static authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Hardware Token-Based Authentication

ID: FedRAMP High IA-5 (11) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Satisfy token quality requirements ↴	CMA_0487 - Satisfy token quality requirements	Manual, Disabled	1.1.0 ↴

# Expiration Of Cached Authenticators

ID: FedRAMP High IA-5 (13) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce expiration of cached authenticators ↴	CMA_C1343 - Enforce expiration of cached authenticators	Manual, Disabled	1.1.0 ↴

# Authenticator Feedback

ID: FedRAMP High IA-6 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Obscure feedback information during authentication process ↴	CMA_C1344 - Obscure feedback information during authentication process	Manual, Disabled	1.1.0 ↴

# Cryptographic Module Authentication

ID: FedRAMP High IA-7 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authenticate to cryptographic module ↗</a>	CMA_0021 - Authenticate to cryptographic module	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Identification And Authentication (Non- Organizational Users)

ID: FedRAMP High IA-8 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Identify and authenticate non- organizational users ↗</a>	CMA_C1346 - Identify and authenticate non-organizational users	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Acceptance Of Piv Credentials From Other Agencies

ID: FedRAMP High IA-8 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accept PIV credentials ↗</a>	CMA_C1347 - Accept PIV credentials	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Acceptance Of Third-Party Credentials

ID: FedRAMP High IA-8 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accept only FICAM-approved third-party credentials ↗</a>	CMA_C1348 - Accept only FICAM-approved third-party credentials	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Use Of Ficam-Approved Products

ID: FedRAMP High IA-8 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ FICAM-approved resources to accept third-party credentials ↗</a>	CMA_C1349 - Employ FICAM-approved resources to accept third-party credentials	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Use Of Ficam-Issued Profiles

ID: FedRAMP High IA-8 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Conform to FICAM-issued profiles ↗</a>	CMA_C1350 - Conform to FICAM-issued profiles	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Incident Response

### Incident Response Policy And Procedures

ID: FedRAMP High IR-1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update incident response policies and procedures ↗</a>	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

### Incident Response Training

ID: FedRAMP High IR-2 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗

## Simulated Events

ID: FedRAMP High IR-2 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Incorporate simulated events into incident response training ↗	CMA_C1356 - Incorporate simulated events into incident response training	Manual, Disabled	1.1.0 ↗

## Automated Training Environments

ID: FedRAMP High IR-2 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ automated training environment ↗	CMA_C1357 - Employ automated training environment	Manual, Disabled	1.1.0 ↗

## Incident Response Testing

ID: FedRAMP High IR-3 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct incident response testing ↗	CMA_0060 - Conduct incident response testing	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish an information security program ↗</a>	CMA_0263 - Establish an information security program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Run simulation attacks ↗</a>	CMA_0486 - Run simulation attacks	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Coordination With Related Plans

ID: FedRAMP High IR-3 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Conduct incident response testing ↗</a>	CMA_0060 - Conduct incident response testing	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish an information security program ↗</a>	CMA_0263 - Establish an information security program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Run simulation attacks ↗</a>	CMA_0486 - Run simulation attacks	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Incident Handling

ID: FedRAMP High IR-4 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess information security events ↗</a>	CMA_0013 - Assess information security events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>

<b>Name</b> <b>should be</b> <b>(Azure portal)</b> <b>enabled</b> ↴	<b>Description</b> vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	<b>Effect(s)</b>	<b>Version</b> (GitHub)
Azure Defender for DNS should be enabled ↴	<p>Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> .</p> <p>Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .</p>	AuditIfNotExists, Disabled	1.0.0 ↴
Azure Defender for Key Vault should be enabled ↴	<p>Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.</p>	AuditIfNotExists, Disabled	1.0.3 ↴
Azure Defender for Resource Manager should be enabled ↴	<p>Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .</p>	AuditIfNotExists, Disabled	1.0.0 ↴
Azure Defender for servers should be enabled ↴	<p>Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.</p>	AuditIfNotExists, Disabled	1.0.3 ↴
Azure Defender for SQL servers on machines should be enabled ↴	<p>Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.</p>	AuditIfNotExists, Disabled	1.0.2 ↴
Azure Defender for SQL should be enabled for unprotected	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	2.0.1 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure SQL servers ↗			
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↗
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Develop security safeguards ↗	CMA_0161 - Develop security safeguards	Manual, Disabled	1.1.0 ↗
Email notification for high severity alerts should be enabled ↗	To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, enable email notifications for high severity alerts in Security Center.	AuditIfNotExists, Disabled	1.0.1 ↗
Email notification to subscription owner for high severity alerts should be enabled ↗	To ensure your subscription owners are notified when there is a potential security breach in their subscription, set email notifications to subscription owners for high severity alerts in Security Center.	AuditIfNotExists, Disabled	2.0.0 ↗
Enable network protection ↗	CMA_0238 - Enable network protection	Manual, Disabled	1.1.0 ↗
Eradicate contaminated information ↗	CMA_0253 - Eradicate contaminated information	Manual, Disabled	1.1.0 ↗
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	1.1.0 ↗
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Maintain incident response plan ↴	CMA_0352 - Maintain incident response plan	Manual, Disabled	1.1.0 ↴
Microsoft Defender for Containers should be enabled ↴	Microsoft Defender for Containers provides hardening, vulnerability assessment and runtime protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	1.0.0 ↴
Microsoft Defender for Storage should be enabled ↴	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	1.0.0 ↴
Perform a trend analysis on threats ↴	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↴
Subscriptions should have a contact email address for security issues ↴	To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, set a security contact to receive email notifications from Security Center.	AuditIfNotExists, Disabled	1.0.1 ↴
View and investigate restricted users ↴	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↴

## Automated Incident Handling Processes

ID: FedRAMP High IR-4 (1) Ownership: Shared

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop an incident response plan ↴	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Enable network protection ↗</a>	CMA_0238 - Enable network protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement incident handling ↗</a>	CMA_0318 - Implement incident handling	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Dynamic Reconfiguration

ID: FedRAMP High IR-4 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Include dynamic reconfig of customer deployed resources ↗</a>	CMA_C1364 - Include dynamic reconfig of customer deployed resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Continuity Of Operations

ID: FedRAMP High IR-4 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Identify classes of Incidents and Actions taken ↗</a>	CMA_C1365 - Identify classes of Incidents and Actions taken	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information Correlation

ID: FedRAMP High IR-4 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗

## Insider Threats - Specific Capabilities

ID: FedRAMP High IR-4 (6) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement Incident handling capability ↗	CMA_C1367 - Implement Incident handling capability	Manual, Disabled	1.1.0 ↗

## Correlation With External Organizations

ID: FedRAMP High IR-4 (8) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Coordinate with external organizations to achieve cross org perspective ↗	CMA_C1368 - Coordinate with external organizations to achieve cross org perspective	Manual, Disabled	1.1.0 ↗

## Incident Monitoring

ID: FedRAMP High IR-5 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for App Service should be enabled ↗	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	1.0.3 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Resource Manager should be enabled ↗</a>	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for servers should be enabled ↗</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for SQL servers on machines should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>

<b>Name</b>  (Azure portal)	<b>Description</b>	<b>Effect(s)</b>  (GitHub)	<b>Version</b>
<a href="#">Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗</a>	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗</a>	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Email notification for high severity alerts should be enabled ↗</a>	To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, enable email notifications for high severity alerts in Security Center.	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Email notification to subscription owner for high severity alerts should be enabled ↗</a>	To ensure your subscription owners are notified when there is a potential security breach in their subscription, set email notifications to subscription owners for high severity alerts in Security Center.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Microsoft Defender for Containers should be enabled ↗</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Subscriptions should have a</a>	To ensure the relevant people in your organization are notified when there is a	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">contact email address for security issues ↗</a>	potential security breach in one of your subscriptions, set a security contact to receive email notifications from Security Center.		

## Automated Reporting

ID: FedRAMP High IR-6 (1) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">Document security operations ↗</a>	CMA_0202 - Document security operations	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Incident Response Assistance

ID: FedRAMP High IR-7 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">Document security operations ↗</a>	CMA_0202 - Document security operations	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automation Support For Availability Of Information / Support

ID: FedRAMP High IR-7 (1) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">Develop an incident response plan ↗</a>	CMA_0145 - Develop an incident response plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enable network protection ↗	CMA_0238 - Enable network protection	Manual, Disabled	1.1.0 ↗
Eradicate contaminated information ↗	CMA_0253 - Eradicate contaminated information	Manual, Disabled	1.1.0 ↗
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	1.1.0 ↗
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

## Coordination With External Providers

ID: FedRAMP High IR-7 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish relationship between incident response capability and external providers ↗	CMA_C1376 - Establish relationship between incident response capability and external providers	Manual, Disabled	1.1.0 ↗
Identify incident response personnel ↗	CMA_0301 - Identify incident response personnel	Manual, Disabled	1.1.0 ↗

## Incident Response Plan

ID: FedRAMP High IR-8 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess information security events ↗	CMA_0013 - Assess information security events	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗
Maintain data breach records ↗	CMA_0351 - Maintain data breach records	Manual, Disabled	1.1.0 ↗
Maintain incident response plan ↗	CMA_0352 - Maintain incident response plan	Manual, Disabled	1.1.0 ↗
Protect incident response plan ↗	CMA_0405 - Protect incident response plan	Manual, Disabled	1.1.0 ↗

## Information Spillage Response

ID: FedRAMP High IR-9 Ownership: Shared

↔ Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Alert personnel of information spillage ↗	CMA_0007 - Alert personnel of information spillage	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Eradicate contaminated information ↗	CMA_0253 - Eradicate contaminated information	Manual, Disabled	1.1.0 ↗
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	1.1.0 ↗
Identify contaminated systems and components ↗	CMA_0300 - Identify contaminated systems and components	Manual, Disabled	1.1.0 ↗
Identify spilled information ↗	CMA_0303 - Identify spilled information	Manual, Disabled	1.1.0 ↗
Isolate information spills ↗	CMA_0346 - Isolate information	Manual,	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
	spills	Disabled	

## Responsible Personnel

ID: FedRAMP High IR-9 (1) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Identify incident response personnel ↗</a>	CMA_0301 - Identify incident response personnel	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Training

ID: FedRAMP High IR-9 (2) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Provide information spillage training ↗</a>	CMA_0413 - Provide information spillage training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Post-Spill Operations

ID: FedRAMP High IR-9 (3) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Develop spillage response procedures ↗</a>	CMA_0162 - Develop spillage response procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Exposure To Unauthorized Personnel

ID: FedRAMP High IR-9 (4) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop security safeguards ↗</a>	CMA_0161 - Develop security safeguards	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Maintenance

### System Maintenance Policy And Procedures

ID: FedRAMP High MA-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update system maintenance policies and procedures ↗</a>	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

### Controlled Maintenance

ID: FedRAMP High MA-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ a media sanitization mechanism ↗</a>	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
activities			

## Automated Maintenance Activities

ID: FedRAMP High MA-2 (2) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Automate remote maintenance activities ↗</a>	CMA_C1402 - Automate remote maintenance activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Produce complete records of remote maintenance activities ↗</a>	CMA_C1403 - Produce complete records of remote maintenance activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Maintenance Tools

ID: FedRAMP High MA-3 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Inspect Tools

ID: FedRAMP High MA-3 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Inspect Media

ID: FedRAMP High MA-3 (2) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Prevent Unauthorized Removal

ID: FedRAMP High MA-3 (3) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ a media sanitization mechanism ↗</a>	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
activities			

## Nonlocal Maintenance

ID: FedRAMP High MA-4 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Document Nonlocal Maintenance

ID: FedRAMP High MA-4 (2) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Comparable Security / Sanitization

ID: FedRAMP High MA-4 (3) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Perform all non-local maintenance ↗</a>	CMA_C1417 - Perform all non-local maintenance	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Cryptographic Protection

ID: FedRAMP High MA-4 (6) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement cryptographic mechanisms ↗	CMA_C1419 - Implement cryptographic mechanisms	Manual, Disabled	1.1.0 ↗

# Maintenance Personnel

ID: FedRAMP High MA-5 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Designate personnel to supervise unauthorized maintenance activities ↗	CMA_C1422 - Designate personnel to supervise unauthorized maintenance activities	Manual, Disabled	1.1.0 ↗
Maintain list of authorized remote maintenance personnel ↗	CMA_C1420 - Maintain list of authorized remote maintenance personnel	Manual, Disabled	1.1.0 ↗
Manage maintenance personnel ↗	CMA_C1421 - Manage maintenance personnel	Manual, Disabled	1.1.0 ↗

# Individuals Without Appropriate Access

ID: FedRAMP High MA-5 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗

## Timely Maintenance

ID: FedRAMP High MA-6 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide timely maintenance support ↗	CMA_C1425 - Provide timely maintenance support	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Media Protection

### Media Protection Policy And Procedures

ID: FedRAMP High MP-1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update media protection policies and procedures ↗	CMA_C1427 - Review and update media protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Media Access

ID: FedRAMP High MP-2 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Media Marking

ID: FedRAMP High MP-3 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Media Storage

ID: FedRAMP High MP-4 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ a media sanitization mechanism ↗</a>	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Media Transport

ID: FedRAMP High MP-5 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage the transportation of assets ↗</a>	CMA_0370 - Manage the transportation of assets	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Cryptographic Protection

ID: FedRAMP High MP-5 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗

## Media Sanitization

ID: FedRAMP High MP-6 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗

## Review / Approve / Track / Document / Verify

ID: FedRAMP High MP-6 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗

## Equipment Testing

ID: FedRAMP High MP-6 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Media Use

ID: FedRAMP High MP-7 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Restrict media use ↗	CMA_0450 - Restrict media use	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Prohibit Use Without Owner

ID: FedRAMP High MP-7 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Restrict media use ↗</a>	CMA_0450 - Restrict media use	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Physical And Environmental Protection

### Physical And Environmental Protection Policy And Procedures

ID: FedRAMP High PE-1 Ownership: Shared

[\[\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Review and update physical and environmental policies and procedures ↗</a>	CMA_C1446 - Review and update physical and environmental policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Physical Access Authorizations

ID: FedRAMP High PE-2 Ownership: Shared

[\[\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Physical Access Control

ID: FedRAMP High PE-3 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define a physical key management process ↗</a>	CMA_0115 - Define a physical key management process	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and maintain an asset inventory ↗</a>	CMA_0266 - Establish and maintain an asset inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Access Control For Transmission Medium

ID: FedRAMP High PE-4 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Access Control For Output Devices

ID: FedRAMP High PE-5 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and</a>	CMA_0323 - Implement physical security for offices, working areas,	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">secure areas ↗</a>	and secure areas		
<a href="#">Manage the input, output, processing, and storage of data ↗</a>	CMA_0369 - Manage the input, output, processing, and storage of data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Intrusion Alarms / Surveillance Equipment

ID: FedRAMP High PE-6 (1) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Install an alarm system ↗</a>	CMA_0338 - Install an alarm system	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage a secure surveillance camera system ↗</a>	CMA_0354 - Manage a secure surveillance camera system	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Visitor Access Records

ID: FedRAMP High PE-8 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Emergency Lighting

ID: FedRAMP High PE-12 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ automatic emergency lighting ↗</a>	CMA_0209 - Employ automatic emergency lighting	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Fire Protection

ID: FedRAMP High PE-13 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Detection Devices / Systems

ID: FedRAMP High PE-13 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement a penetration testing methodology ↗</a>	CMA_0306 - Implement a penetration testing methodology	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Run simulation attacks ↗</a>	CMA_0486 - Run simulation attacks	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Suppression Devices / Systems

ID: FedRAMP High PE-13 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automatic Fire Suppression

ID: FedRAMP High PE-13 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Temperature And Humidity Controls

ID: FedRAMP High PE-14 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Monitoring With Alarms / Notifications

ID: FedRAMP High PE-14 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Install an alarm system ↗	CMA_0338 - Install an alarm system	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Water Damage Protection

ID: FedRAMP High PE-15 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Delivery And Removal

ID: FedRAMP High PE-16 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define requirements for managing assets ↗	CMA_0125 - Define requirements for managing assets	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Alternate Work Site

ID: FedRAMP High PE-17 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure alternate work sites ↗	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Location Of Information System Components

ID: FedRAMP High PE-18 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Planning

### Security Planning Policy And Procedures

ID: FedRAMP High PL-1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update planning policies and procedures ↗	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## System Security Plan

ID: FedRAMP High PL-2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	1.1.0 ↗
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	1.1.0 ↗
Develop SSP that meets criteria ↗	CMA_C1492 - Develop SSP that meets criteria	Manual, Disabled	1.1.0 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	1.1.0 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗

## Plan / Coordinate With Other Organizational Entities

ID: FedRAMP High PL-2 (3) Ownership: Shared

↔ Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	1.1.0 ↗
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	1.1.0 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗

## Rules Of Behavior

ID: FedRAMP High PL-4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop acceptable use policies and procedures ↗	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce rules of behavior and access agreements ↗	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Social Media And Networking Restrictions

ID: FedRAMP High PL-4 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop acceptable use policies and procedures ↗	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information Security Architecture

ID: FedRAMP High PL-8 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop a concept of operations (CONOPS) ↗	CMA_0141 - Develop a concept of operations (CONOPS)	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update the information security architecture ↗	CMA_C1504 - Review and update the information security architecture	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Personnel Security

### Personnel Security Policy And Procedures

ID: FedRAMP High PS-1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update personnel security policies and procedures ↗	CMA_C1507 - Review and update personnel security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

### Position Risk Designation

ID: FedRAMP High PS-2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign risk designations ↗	CMA_0016 - Assign risk designations	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Personnel Screening

ID: FedRAMP High PS-3 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Clear personnel with access to classified information ↗	CMA_0054 - Clear personnel with access to classified information	Manual, Disabled	1.1.0 ↗
Implement personnel screening ↗	CMA_0322 - Implement personnel screening	Manual, Disabled	1.1.0 ↗
Rescreen individuals at a defined frequency ↗	CMA_C1512 - Rescreen individuals at a defined frequency	Manual, Disabled	1.1.0 ↗

## Information With Special Protection Measures

ID: FedRAMP High PS-3 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Protect special information ↗	CMA_0409 - Protect special information	Manual, Disabled	1.1.0 ↗

## Personnel Termination

ID: FedRAMP High PS-4 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct exit interview upon termination ↗	CMA_0058 - Conduct exit interview upon termination	Manual, Disabled	1.1.0 ↗
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	1.1.0 ↗
Notify upon termination or transfer ↗	CMA_0381 - Notify upon termination or transfer	Manual, Disabled	1.1.0 ↗
Protect against and prevent data theft from departing employees ↗	CMA_0398 - Protect against and prevent data theft from departing employees	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Retain terminated user data ↗</a>	CMA_0455 - Retain terminated user data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Notification

ID: FedRAMP High PS-4 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Automate notification of employee termination ↗</a>	CMA_C1521 - Automate notification of employee termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Personnel Transfer

ID: FedRAMP High PS-5 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Initiate transfer or reassignment actions ↗</a>	CMA_0333 - Initiate transfer or reassignment actions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Modify access authorizations upon personnel transfer ↗</a>	CMA_0374 - Modify access authorizations upon personnel transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Notify upon termination or transfer ↗</a>	CMA_0381 - Notify upon termination or transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Reevaluate access upon personnel transfer ↗</a>	CMA_0424 - Reevaluate access upon personnel transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Access Agreements

ID: FedRAMP High PS-6 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document organizational access agreements ↗	CMA_0192 - Document organizational access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce rules of behavior and access agreements ↗	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Ensure access agreements are signed or resigned timely ↗	CMA_C1528 - Ensure access agreements are signed or resigned timely	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require users to sign access agreement ↗	CMA_0440 - Require users to sign access agreement	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update organizational access agreements ↗	CMA_0520 - Update organizational access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Third-Party Personnel Security

ID: FedRAMP High PS-7 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document third-party personnel security requirements ↗	CMA_C1531 - Document third-party personnel security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require notification of third-party personnel transfer or termination ↗	CMA_C1532 - Require notification of third-party personnel transfer or termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require third-party providers to comply with personnel security policies and procedures ↗	CMA_C1530 - Require third-party providers to comply with personnel security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Personnel Sanctions

ID: FedRAMP High PS-8 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement formal sanctions process ↗</a>	CMA_0317 - Implement formal sanctions process	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Notify personnel upon sanctions ↗</a>	CMA_0380 - Notify personnel upon sanctions	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Risk Assessment

### Risk Assessment Policy And Procedures

ID: FedRAMP High RA-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update risk assessment policies and procedures ↗</a>	CMA_C1537 - Review and update risk assessment policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Categorization

ID: FedRAMP High RA-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Categorize information ↗</a>	CMA_0052 - Categorize information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop business classification schemes ↗</a>	CMA_0155 - Develop business classification schemes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Ensure security categorization is approved ↗</a>	CMA_C1540 - Ensure security categorization is approved	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review label activity and analytics ↗	CMA_0474 - Review label activity and analytics	Manual, Disabled	1.1.0 ↗

## Risk Assessment

ID: FedRAMP High RA-3 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct Risk Assessment ↗	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	1.1.0 ↗
Conduct risk assessment and distribute its results ↗	CMA_C1544 - Conduct risk assessment and distribute its results	Manual, Disabled	1.1.0 ↗
Conduct risk assessment and document its results ↗	CMA_C1542 - Conduct risk assessment and document its results	Manual, Disabled	1.1.0 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	1.1.0 ↗

## Vulnerability Scanning

ID: FedRAMP High RA-5 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
A vulnerability assessment solution should be enabled on your virtual machines ↗	Audits virtual machines to detect whether they are running a supported vulnerability assessment solution. A core component of every cyber risk and security program is the identification and analysis of vulnerabilities. Azure Security Center's standard pricing tier includes vulnerability scanning for your virtual machines at no extra cost. Additionally, Security Center can automatically deploy this tool for you.	AuditIfNotExists, Disabled	3.0.0 ↗

<b>Name</b>  (Azure portal)	<b>Description</b>	<b>Effect(s)</b>  (GitHub)	<b>Version</b>
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Resource Manager should be enabled ↗</a>	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for servers should be enabled ↗</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for SQL servers on machines should be enabled ↴	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↴	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↴	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Container registry images should have vulnerability findings resolved ↴	Container image vulnerability assessment scans your registry for security vulnerabilities and exposes detailed findings for each image.  Resolving the vulnerabilities can greatly improve your containers' security posture and protect them from attacks.	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
Microsoft Defender for Containers should be enabled ↴	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
Microsoft Defender for Storage should be enabled ↴	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption.  The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
Perform vulnerability scans ↴	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Remediate information	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">system flaws ↗</a>			
<a href="#">SQL databases should have vulnerability findings resolved ↗</a>	Monitor vulnerability assessment scan results and recommendations for how to remediate database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">4.1.0 ↗</a>
<a href="#">SQL servers on machines should have vulnerability findings resolved ↗</a>	SQL vulnerability assessment scans your database for security vulnerabilities, and exposes any deviations from best practices such as misconfigurations, excessive permissions, and unprotected sensitive data. Resolving the vulnerabilities found can greatly improve your database security posture.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Vulnerabilities in container security configurations should be remediated ↗</a>	Audit vulnerabilities in security configuration on machines with Docker installed and display as recommendations in Azure Security Center.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Vulnerabilities in security configuration on your machines should be remediated ↗</a>	Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
<a href="#">Vulnerabilities in security configuration on your virtual machine scale sets should be remediated ↗</a>	Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Vulnerability assessment should be enabled on SQL Managed Instance ↗</a>	Audit each SQL Managed Instance which doesn't have recurring vulnerability assessment scans enabled. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Vulnerability assessment should be enabled on your SQL servers ↗</a>	Audit Azure SQL servers which do not have vulnerability assessment properly configured. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Vulnerability assessment should be enabled on your Synapse workspaces ↗	Discover, track, and remediate potential vulnerabilities by configuring recurring SQL vulnerability assessment scans on your Synapse workspaces.	AuditIfNotExists, Disabled	1.0.0 ↗

## Update Tool Capability

ID: FedRAMP High RA-5 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗

## Update By Frequency / Prior To New Scan / When Identified

ID: FedRAMP High RA-5 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗

## Breadth / Depth Of Coverage

ID: FedRAMP High RA-5 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Perform vulnerability scans ↗</a>	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Discoverable Information

ID: FedRAMP High RA-5 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Take action in response to customer information ↗</a>	CMA_C1554 - Take action in response to customer information	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Privileged Access

ID: FedRAMP High RA-5 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement privileged access for executing vulnerability scanning activities ↗</a>	CMA_C1555 - Implement privileged access for executing vulnerability scanning activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Trend Analyses

ID: FedRAMP High RA-5 (6) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Observe and report security weaknesses ↗	CMA_0384 - Observe and report security weaknesses	Manual, Disabled	1.1.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Perform threat modeling ↗	CMA_0392 - Perform threat modeling	Manual, Disabled	1.1.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗

## Review Historic Audit Logs

ID: FedRAMP High RA-5 (8) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit privileged functions ↗	CMA_0019 - Audit privileged functions	Manual, Disabled	1.1.0 ↗
Audit user account status ↗	CMA_0020 - Audit user account status	Manual, Disabled	1.1.0 ↗
Correlate audit records ↗	CMA_0087 - Correlate audit records	Manual, Disabled	1.1.0 ↗
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↗
Establish requirements for audit review and reporting ↗	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	1.1.0 ↗
Integrate audit review, analysis, and reporting ↗	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	1.1.0 ↗
Integrate cloud app security with a siem ↗	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	1.1.0 ↗
Review account provisioning	CMA_0460 - Review account	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">logs ↗</a>	provisioning logs	Disabled	
<a href="#">Review administrator assignments weekly ↗</a>	CMA_0461 - Review administrator assignments weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review audit data ↗</a>	CMA_0466 - Review audit data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review cloud identity report overview ↗</a>	CMA_0468 - Review cloud identity report overview	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review controlled folder access events ↗</a>	CMA_0471 - Review controlled folder access events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review exploit protection events ↗</a>	CMA_0472 - Review exploit protection events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review file and folder activity ↗</a>	CMA_0473 - Review file and folder activity	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review role group changes weekly ↗</a>	CMA_0476 - Review role group changes weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Correlate Scanning Information

ID: FedRAMP High RA-5 (10) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Correlate Vulnerability scan information ↗</a>	CMA_C1558 - Correlate Vulnerability scan information	Manual, Disabled	<a href="#">1.1.1 ↗</a>

## System And Services Acquisition

### System And Services Acquisition Policy And Procedures

ID: FedRAMP High SA-1 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update system and services acquisition policies and procedures ↴	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	1.1.0 ↴

## Allocation Of Resources

ID: FedRAMP High SA-2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Align business objectives and IT goals ↴	CMA_0008 - Align business objectives and IT goals	Manual, Disabled	1.1.0 ↴
Allocate resources in determining information system requirements ↴	CMA_C1561 - Allocate resources in determining information system requirements	Manual, Disabled	1.1.0 ↴
Establish a discrete line item in budgeting documentation ↴	CMA_C1563 - Establish a discrete line item in budgeting documentation	Manual, Disabled	1.1.0 ↴
Establish a privacy program ↴	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↴
Govern the allocation of resources ↴	CMA_0293 - Govern the allocation of resources	Manual, Disabled	1.1.0 ↴
Secure commitment from leadership ↴	CMA_0489 - Secure commitment from leadership	Manual, Disabled	1.1.0 ↴

## System Development Life Cycle

ID: FedRAMP High SA-3 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define information security roles	CMA_C1565 - Define information	Manual,	1.1.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">and responsibilities ↗</a>	security roles and responsibilities	Disabled	
<a href="#">Identify individuals with security roles and responsibilities ↗</a>	CMA_C1566 - Identify individuals with security roles and responsibilities	Manual, Disabled	<a href="#">1.1.1 ↗</a>
<a href="#">Integrate risk management process into SDLC ↗</a>	CMA_C1567 - Integrate risk management process into SDLC	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Acquisition Process

ID: FedRAMP High SA-4 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Determine supplier contract obligations ↗</a>	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document acquisition contract acceptance criteria ↗</a>	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document protection of personal data in acquisition contracts ↗</a>	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document protection of security information in acquisition contracts ↗</a>	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document requirements for the use of shared data in contracts ↗</a>	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security assurance requirements in acquisition contracts ↗</a>	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security documentation requirements in acquisition contract ↗</a>	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security functional requirements in acquisition</a>	CMA_0201 - Document security functional requirements in	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">contracts ↗</a>	acquisition contracts		
<a href="#">Document security strength requirements in acquisition contracts ↗</a>	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document the information system environment in acquisition contracts ↗</a>	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document the protection of cardholder data in third party contracts ↗</a>	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Functional Properties Of Security Controls

ID: FedRAMP High SA-4 (1) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Obtain functional properties of security controls ↗</a>	CMA_C1575 - Obtain functional properties of security controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Design / Implementation Information For Security Controls

ID: FedRAMP High SA-4 (2) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Obtain design and implementation information for the security controls ↗</a>	CMA_C1576 - Obtain design and implementation information for the security controls	Manual, Disabled	<a href="#">1.1.1 ↗</a>

## Continuous Monitoring Plan

ID: FedRAMP High SA-4 (8) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Obtain continuous monitoring plan for security controls ↗</a>	CMA_C1577 - Obtain continuous monitoring plan for security controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Functions / Ports / Protocols / Services In Use

ID: FedRAMP High SA-4 (9) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Require developer to identify SDLC ports, protocols, and services ↗</a>	CMA_C1578 - Require developer to identify SDLC ports, protocols, and services	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Use Of Approved Piv Products

ID: FedRAMP High SA-4 (10) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ FIPS 201-approved technology for PIV ↗</a>	CMA_C1579 - Employ FIPS 201-approved technology for PIV	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information System Documentation

ID: FedRAMP High SA-5 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Distribute information system documentation ↗	CMA_C1584 - Distribute information system documentation	Manual, Disabled	1.1.0 ↗
Document customer-defined actions ↗	CMA_C1582 - Document customer-defined actions	Manual, Disabled	1.1.0 ↗
Obtain Admin documentation ↗	CMA_C1580 - Obtain Admin documentation	Manual, Disabled	1.1.0 ↗
Obtain user security function documentation ↗	CMA_C1581 - Obtain user security function documentation	Manual, Disabled	1.1.0 ↗
Protect administrator and user documentation ↗	CMA_C1583 - Protect administrator and user documentation	Manual, Disabled	1.1.0 ↗

## External Information System Services

ID: FedRAMP High SA-9 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define and document government oversight ↗	CMA_C1587 - Define and document government oversight	Manual, Disabled	1.1.0 ↗
Require external service providers to comply with security requirements ↗	CMA_C1586 - Require external service providers to comply with security requirements	Manual, Disabled	1.1.0 ↗
Review cloud service provider's compliance with policies and agreements ↗	CMA_0469 - Review cloud service provider's compliance with policies and agreements	Manual, Disabled	1.1.0 ↗
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	1.1.0 ↗

## Risk Assessments / Organizational Approvals

ID: FedRAMP High SA-9 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess risk in third party relationships ↗	CMA_0014 - Assess risk in third party relationships	Manual, Disabled	1.1.0 ↗
Obtain approvals for acquisitions and outsourcing ↗	CMA_C1590 - Obtain approvals for acquisitions and outsourcing	Manual, Disabled	1.1.0 ↗

## Identification Of Functions / Ports / Protocols / Services

ID: FedRAMP High SA-9 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Identify external service providers ↗	CMA_C1591 - Identify external service providers	Manual, Disabled	1.1.0 ↗

## Consistent Interests Of Consumers And Providers

ID: FedRAMP High SA-9 (4) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure external providers consistently meet interests of the customers ↗	CMA_C1592 - Ensure external providers consistently meet interests of the customers	Manual, Disabled	1.1.0 ↗

## Processing, Storage, And Service Location

ID: FedRAMP High SA-9 (5) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Restrict location of information processing, storage and services ↗	CMA_C1593 - Restrict location of information processing, storage and services	Manual, Disabled	1.1.0 ↗

## Developer Configuration Management

ID: FedRAMP High SA-10 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Address coding vulnerabilities ↗	CMA_0003 - Address coding vulnerabilities	Manual, Disabled	1.1.0 ↗
Develop and document application security requirements ↗	CMA_0148 - Develop and document application security requirements	Manual, Disabled	1.1.0 ↗
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↗
Establish a secure software development program ↗	CMA_0259 - Establish a secure software development program	Manual, Disabled	1.1.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗
Require developers to document approved changes and potential impact ↗	CMA_C1597 - Require developers to document approved changes and potential impact	Manual, Disabled	1.1.0 ↗
Require developers to implement only approved changes ↗	CMA_C1596 - Require developers to implement only approved changes	Manual, Disabled	1.1.0 ↗
Require developers to manage change integrity ↗	CMA_C1595 - Require developers to manage change integrity	Manual, Disabled	1.1.0 ↗

## Software / Firmware Integrity Verification

ID: FedRAMP High SA-10 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Verify software, firmware and information integrity ↗</a>	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Developer Security Testing And Evaluation

ID: FedRAMP High SA-11 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Perform vulnerability scans ↗</a>	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require developers to produce evidence of security assessment plan execution ↗</a>	CMA_C1602 - Require developers to produce evidence of security assessment plan execution	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Supply Chain Protection

ID: FedRAMP High SA-12 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess risk in third party relationships ↗</a>	CMA_0014 - Assess risk in third party relationships	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define requirements for supplying goods and services ↗</a>	CMA_0126 - Define requirements for supplying goods and services	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Determine supplier contract obligations ↗</a>	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish policies for supply chain risk management ↗</a>	CMA_0275 - Establish policies for supply chain risk management	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Development Process, Standards, And Tools

ID: FedRAMP High SA-15 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Review development process, standards and tools ↗</a>	CMA_C1610 - Review development process, standards and tools	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Developer-Provided Training

ID: FedRAMP High SA-16 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Require developers to provide training ↗</a>	CMA_C1611 - Require developers to provide training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Developer Security Architecture And Design

ID: FedRAMP High SA-17 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Require developers to build security architecture ↗</a>	CMA_C1612 - Require developers to build security architecture	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require developers to describe accurate security functionality ↗</a>	CMA_C1613 - Require developers to describe accurate security functionality	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require developers to provide unified security protection approach ↗</a>	CMA_C1614 - Require developers to provide unified security protection approach	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# System And Communications Protection

## System And Communications Protection Policy And Procedures

ID: FedRAMP High SC-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update system and communications protection policies and procedures ↗</a>	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Application Partitioning

ID: FedRAMP High SC-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authorize remote access ↗</a>	CMA_0024 - Authorize remote access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Separate user and information system management functionality ↗</a>	CMA_0493 - Separate user and information system management functionality	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Use dedicated machines for administrative tasks ↗</a>	CMA_0527 - Use dedicated machines for administrative tasks	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Function Isolation

ID: FedRAMP High SC-3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↗
Endpoint protection solution should be installed on virtual machine scale sets ↗	Audit the existence and health of an endpoint protection solution on your virtual machines scale sets, to protect them from threats and vulnerabilities.	AuditIfNotExists, Disabled	3.0.0 ↗
Monitor missing Endpoint Protection in Azure Security Center ↗	Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.0.0 ↗
Windows Defender Exploit Guard should be enabled on your machines ↗	Windows Defender Exploit Guard uses the Azure Policy Guest Configuration agent. Exploit Guard has four components that are designed to lock down devices against a wide variety of attack vectors and block behaviors commonly used in malware attacks while enabling enterprises to balance their security risk and productivity requirements (Windows only).	AuditIfNotExists, Disabled	2.0.0 ↗

## Denial Of Service Protection

ID: FedRAMP High SC-5 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure DDoS Protection Standard should be enabled ↗	DDoS protection standard should be enabled for all virtual networks with a subnet that is part of an application gateway with a public IP.	AuditIfNotExists, Disabled	3.0.0 ↗
Azure Web Application Firewall should be enabled for ↗	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized	Audit, Deny, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Front Door entry-points ↗	protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.		
Develop and document a DDoS response plan ↗	CMA_0147 - Develop and document a DDoS response plan	Manual, Disabled	1.1.0 ↗
IP Forwarding on your virtual machine should be disabled ↗	Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely required (e.g., when using the VM as a network virtual appliance), and therefore, this should be reviewed by the network security team.	AuditIfNotExists, Disabled	3.0.0 ↗
Web Application Firewall (WAF) should be enabled for Application Gateway ↗	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.	Audit, Deny, Disabled	2.0.0 ↗

## Resource Availability

ID: FedRAMP High SC-6 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Govern the allocation of resources ↗	CMA_0293 - Govern the allocation of resources	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Manage availability and capacity ↗	CMA_0356 - Manage availability and capacity	Manual, Disabled	1.1.0 ↗
Secure commitment from leadership ↗	CMA_0489 - Secure commitment from leadership	Manual, Disabled	1.1.0 ↗

## Boundary Protection

ID: FedRAMP High SC-7 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: All Internet traffic should be routed via your deployed Azure Firewall ↗	Azure Security Center has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall	AuditIfNotExists, Disabled	3.0.0-preview ↗
[Preview]: Storage account public access should be disallowed ↗	Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it.	audit, Audit, deny, Deny, disabled, Disabled	3.1.0-preview ↗
Adaptive network hardening recommendations should be applied on internet facing virtual machines ↗	Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface	AuditIfNotExists, Disabled	3.0.0 ↗
All network ports should be restricted on network security groups associated	Azure Security Center has identified some of your network security groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.	AuditIfNotExists, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">to your virtual machine ↗</a>			
<a href="#">API Management services should use a virtual network ↗</a>	Azure Virtual Network deployment provides enhanced security, isolation and allows you to place your API Management service in a non-internet routable network that you control access to. These networks can then be connected to your on-premises networks using various VPN technologies, which enables access to your backend services within the network and/or on-premises. The developer portal and API gateway, can be configured to be accessible either from the Internet or only within the virtual network.	Audit, Deny, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">App Configuration should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Authorized IP ranges should be defined on Kubernetes Services ↗</a>	Restrict access to the Kubernetes Service Management API by granting API access only to IP addresses in specific ranges. It is recommended to limit access to authorized IP ranges to ensure that only applications from allowed networks can access the cluster.	Audit, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Azure API for FHIR should use private link ↗</a>	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> ↗ .	Audit, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Cache for Redis should use private link ↗	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Cognitive Search service should use a SKU that supports private link ↗	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should disable public network access ↗	Disabling public network access improves security by ensuring that your Azure Cognitive Search service is not exposed on the public internet. Creating private endpoints can limit exposure of your Search service. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.	Audit, Disabled	1.0.0 ↗
Azure Cosmos DB accounts should	Firewall rules should be defined on your Azure Cosmos DB accounts to prevent	Audit, Deny, Disabled	2.0.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">have firewall rules</a>	traffic from unauthorized sources. Accounts that have at least one IP rule defined with the virtual network filter enabled are deemed compliant. Accounts disabling public access are also deemed compliant.		
<a href="#">Azure Data Factory should use private link</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a> .	AuditIfNotExists, Disabled	1.0.0
<a href="#">Azure Event Grid domains should use private link</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> .	Audit, Disabled	1.0.2
<a href="#">Azure Event Grid topics should use private link</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> .	Audit, Disabled	1.0.2

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure File Sync should use private link ↗	Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Key Vault should have firewall enabled ↗	Enable the key vault firewall so that the key vault is not accessible by default to any public IPs. Optionally, you can configure specific IP ranges to limit access to those networks. Learn more at: <a href="https://docs.microsoft.com/azure/key-vault/general/network-security">https://docs.microsoft.com/azure/key-vault/general/network-security</a>	Audit, Deny, Disabled	3.2.1 ↗
Azure Key Vaults should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink</a> .	[parameters('audit_effect')]	1.2.1 ↗
Azure Machine Learning workspaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .	Audit, Disabled	1.0.0 ↗
Azure Service Bus namespaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a>.</p>		
<a href="#">Azure SignalR Service should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> ↗.</p>	Audit, Disabled	1.0.0 ↗
<a href="#">Azure Synapse workspaces should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a>.</p>	Audit, Disabled	1.0.1 ↗
<a href="#">Azure Web Application Firewall should be enabled for Azure Front Door entry-points ↗</a>	<p>Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.</p>	Audit, Deny, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Web PubSub Service should use private link ↗	<p>Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks.</p> <p>Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a>.</p>	Audit, Disabled	1.0.0 ↗
Cognitive Services accounts should disable public network access ↗	<p>To improve the security of Cognitive Services accounts, ensure that it isn't exposed to the public internet and can only be accessed from a private endpoint. Disable the public network access property as described in <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a>. This option disables access from any public address space outside the Azure IP range, and denies all logins that match IP or virtual network-based firewall rules. This reduces data leakage risks.</p>	Audit, Deny, Disabled	3.0.1 ↗
Cognitive Services accounts should restrict network access ↗	<p>Network access to Cognitive Services accounts should be restricted. Configure network rules so only applications from allowed networks can access the Cognitive Services account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges.</p>	Audit, Deny, Disabled	3.0.0 ↗
Cognitive Services should use private link ↗	<p>Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage.</p> <p>Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a>.</p>	Audit, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p><a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a>.</p>		
Container registries should not allow unrestricted network access <a href="#">♂</a>	<p>Azure container registries by default accept connections over the internet from hosts on any network. To protect your registries from potential threats, allow access from only specific private endpoints, public IP addresses or address ranges. If your registry doesn't have network rules configured, it will appear in the unhealthy resources. Learn more about Container Registry network rules here:</p> <p><a href="https://aka.ms/acr/privatelink">https://aka.ms/acr/privatelink</a>, <a href="https://aka.ms/acr/portal/public-network">https://aka.ms/acr/portal/public-network</a> and <a href="https://aka.ms/acr/vnet">https://aka.ms/acr/vnet</a>.</p>	Audit, Deny, Disabled	2.0.0 <a href="#">♂</a>
Container registries should use private link <a href="#">♂</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a>.</p>	Audit, Disabled	1.0.1 <a href="#">♂</a>
CosmosDB accounts should use private link <a href="#">♂</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at:</p> <p><a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a>.</p>	Audit, Disabled	1.0.0 <a href="#">♂</a>
Disk access resources should use private link <a href="#">♂</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the</p>	AuditIfNotExists, Disabled	1.0.0 <a href="#">♂</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a>.</p>		
<a href="#">Event Hub namespaces should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a>.</p>	AuditIfNotExists, Disabled	1.0.0 ↗
<a href="#">Implement system boundary protection ↗</a>	CMA_0328 - Implement system boundary protection	Manual, Disabled	1.1.0 ↗
<a href="#">Internet-facing virtual machines should be protected with network security groups ↗</a>	<p>Protect your virtual machines from potential threats by restricting access to them with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsg-doc">https://aka.ms/nsg-doc</a>.</p>	AuditIfNotExists, Disabled	3.0.0 ↗
<a href="#">IoT Hub device provisioning service instances should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a>.</p>	Audit, Disabled	1.0.0 ↗
<a href="#">IP Forwarding on your virtual machine should be disabled ↗</a>	Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely required (e.g., when using the VM as a network virtual appliance), and therefore,	AuditIfNotExists, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	this should be reviewed by the network security team.		
Management ports of virtual machines should be protected with just-in-time network access control ↗	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.0.0 ↗
Management ports should be closed on your virtual machines ↗	Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine.	AuditIfNotExists, Disabled	3.0.0 ↗
Non-internet-facing virtual machines should be protected with network security groups ↗	Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsq-doc">https://aka.ms/nsq-doc</a> ↗	AuditIfNotExists, Disabled	3.0.0 ↗
Private endpoint connections on Azure SQL Database should be enabled ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↗
Private endpoint should be enabled for MariaDB servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for MySQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Private endpoint should be enabled for PostgreSQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Public network access on Azure SQL Database should be disabled ↗	Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP or virtual network based firewall rules.	Audit, Deny, Disabled	1.1.0 ↗
Public network access should be disabled for MariaDB servers ↗	Disable the public network access property to improve security and ensure your Azure Database for MariaDB can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↗
Public network access should be disabled for MySQL servers ↗	Disable the public network access property to improve security and ensure your Azure Database for MySQL can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↗
Public network access should be disabled for PostgreSQL servers ↗	Disable the public network access property to improve security and ensure your Azure Database for PostgreSQL can only be accessed from a private endpoint. This configuration disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.1 ↗
Storage accounts should restrict network access ↗	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow	Audit, Deny, Disabled	1.1.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges		
<a href="#">Storage accounts should restrict network access using virtual network rules ↗</a>	Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.	Audit, Deny, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Storage accounts should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview ↗</a>	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Subnets should be associated with a Network Security Group ↗</a>	Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">VM Image Builder templates should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .	Audit, Disabled, Deny	<a href="#">1.1.0 ↗</a>
<a href="#">Web Application Firewall (WAF) should be</a>	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">enabled for Application Gateway ↗</a>	incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.		

## Access Points

ID: FedRAMP High SC-7 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Preview]: All Internet traffic should be routed via your deployed Azure Firewall ↗</a>	Azure Security Center has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall	AuditIfNotExists, Disabled	<a href="#">3.0.0-preview ↗</a>
<a href="#">[Preview]: Storage account public access should be disallowed ↗</a>	Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it.	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">3.1.0-preview ↗</a>
<a href="#">Adaptive network hardening recommendations should be applied on internet facing virtual machines ↗</a>	Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">All network ports should be restricted on</a>	Azure Security Center has identified some of your network security groups' inbound rules to be too permissive. Inbound rules	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">network security groups associated to your virtual machine ↗</a>	should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.		
<a href="#">API Management services should use a virtual network ↗</a>	Azure Virtual Network deployment provides enhanced security, isolation and allows you to place your API Management service in a non-internet routable network that you control access to. These networks can then be connected to your on-premises networks using various VPN technologies, which enables access to your backend services within the network and/or on-premises. The developer portal and API gateway, can be configured to be accessible either from the Internet or only within the virtual network.	Audit, Deny, Disabled	1.0.2 ↗
<a href="#">App Configuration should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> ↗ .	AuditIfNotExist, Disabled	1.0.2 ↗
<a href="#">Authorized IP ranges should be defined on Kubernetes Services ↗</a>	Restrict access to the Kubernetes Service Management API by granting API access only to IP addresses in specific ranges. It is recommended to limit access to authorized IP ranges to ensure that only applications from allowed networks can access the cluster.	Audit, Disabled	2.0.1 ↗
<a href="#">Azure API for FHIR should use private link ↗</a>	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> .		
Azure Cache for Redis should use private link ↗	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Cognitive Search service should use a SKU that supports private link ↗	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should disable public network access ↗	Disabling public network access improves security by ensuring that your Azure Cognitive Search service is not exposed on the public internet. Creating private endpoints can limit exposure of your Search service. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Cosmos DB accounts should have firewall rules ↴	<p>Firewall rules should be defined on your Azure Cosmos DB accounts to prevent traffic from unauthorized sources.</p> <p>Accounts that have at least one IP rule defined with the virtual network filter enabled are deemed compliant. Accounts disabling public access are also deemed compliant.</p>	Audit, Deny, Disabled	2.0.0 ↴
Azure Data Factory should use private link ↴	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at:</p> <p><a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a>.</p>	AuditIfNotExists, Disabled	1.0.0 ↴
Azure Event Grid domains should use private link ↴	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at:</p> <p><a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> ↴.</p>	Audit, Disabled	1.0.2 ↴
Azure Event Grid topics should use private link ↴	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn</p>	Audit, Disabled	1.0.2 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints ↗</a> .		
Azure File Sync should use private link ↗	Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Key Vault should have firewall enabled ↗	Enable the key vault firewall so that the key vault is not accessible by default to any public IPs. Optionally, you can configure specific IP ranges to limit access to those networks. Learn more at: <a href="https://docs.microsoft.com/azure/key-vault/general/network-security">https://docs.microsoft.com/azure/key-vault/general/network-security</a>	Audit, Deny, Disabled	3.2.1 ↗
Azure Key Vaults should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink ↗</a> .	[parameters('audit_effect')]	1.2.1 ↗
Azure Machine Learning workspaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .	Audit, Disabled	1.0.0 ↗
Azure Service Bus namespaces	Azure Private Link lets you connect your virtual network to Azure services without a	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should use private link ↗</a>	public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .		
<a href="#">Azure SignalR Service should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .	Audit, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Synapse workspaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a> .	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Azure Web Application Firewall should be enabled for Azure Front Door entry-points ↗</a>	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by	Audit, Deny, Disabled	<a href="#">1.0.2 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	countries, IP address ranges, and other http(s) parameters via custom rules.		
Azure Web PubSub Service should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a> ↗ .	Audit, Disabled	1.0.0 ↗
Cognitive Services accounts should disable public network access ↗	To improve the security of Cognitive Services accounts, ensure that it isn't exposed to the public internet and can only be accessed from a private endpoint. Disable the public network access property as described in <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> ↗ . This option disables access from any public address space outside the Azure IP range, and denies all logins that match IP or virtual network-based firewall rules. This reduces data leakage risks.	Audit, Deny, Disabled	3.0.1 ↗
Cognitive Services accounts should restrict network access ↗	Network access to Cognitive Services accounts should be restricted. Configure network rules so only applications from allowed networks can access the Cognitive Services account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges.	Audit, Deny, Disabled	3.0.0 ↗
Cognitive Services should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll	Audit, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>reduce the potential for data leakage.</p> <p>Learn more about private links at: <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a>.</p>		
<a href="#">Container registries should not allow unrestricted network access ↗</a>	<p>Azure container registries by default accept connections over the internet from hosts on any network. To protect your registries from potential threats, allow access from only specific private endpoints, public IP addresses or address ranges. If your registry doesn't have network rules configured, it will appear in the unhealthy resources. Learn more about Container Registry network rules here:</p> <p><a href="https://aka.ms/acr/privatelink">https://aka.ms/acr/privatelink</a>,  <a href="https://aka.ms/acr/portal/public-network">https://aka.ms/acr/portal/public-network</a> and <a href="https://aka.ms/acr/vnet">https://aka.ms/acr/vnet</a>.</p>	Audit, Deny, Disabled	2.0.0 ↗
<a href="#">Container registries should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a>.</p>	Audit, Disabled	1.0.1 ↗
<a href="#">CosmosDB accounts should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at:</p> <p><a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a>.</p>	Audit, Disabled	1.0.0 ↗
<a href="#">Disk access resources should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or</p>	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a>.</p>		
<a href="#">Event Hub namespaces should use private link</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a>.</p>	AuditIfNotExists, Disabled	1.0.0 <a href="#">↗</a>
<a href="#">Internet-facing virtual machines should be protected with network security groups</a>	<p>Protect your virtual machines from potential threats by restricting access to them with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsg-doc">https://aka.ms/nsg-doc</a></p>	AuditIfNotExists, Disabled	3.0.0 <a href="#">↗</a>
<a href="#">IoT Hub device provisioning service instances should use private link</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a>.</p>	Audit, Disabled	1.0.0 <a href="#">↗</a>
<a href="#">IP Forwarding on your virtual machine should be disabled</a>	<p>Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely required (e.g., when using the VM as a network virtual appliance), and therefore,</p>	AuditIfNotExists, Disabled	3.0.0 <a href="#">↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	this should be reviewed by the network security team.		
Management ports of virtual machines should be protected with just-in-time network access control ↗	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.0.0 ↗
Management ports should be closed on your virtual machines ↗	Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine.	AuditIfNotExists, Disabled	3.0.0 ↗
Non-internet-facing virtual machines should be protected with network security groups ↗	Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsq-doc">https://aka.ms/nsq-doc</a> ↗	AuditIfNotExists, Disabled	3.0.0 ↗
Private endpoint connections on Azure SQL Database should be enabled ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↗
Private endpoint should be enabled for MariaDB servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for MySQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Private endpoint should be enabled for PostgreSQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Public network access on Azure SQL Database should be disabled ↗	Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP or virtual network based firewall rules.	Audit, Deny, Disabled	1.1.0 ↗
Public network access should be disabled for MariaDB servers ↗	Disable the public network access property to improve security and ensure your Azure Database for MariaDB can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↗
Public network access should be disabled for MySQL servers ↗	Disable the public network access property to improve security and ensure your Azure Database for MySQL can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↗
Public network access should be disabled for PostgreSQL servers ↗	Disable the public network access property to improve security and ensure your Azure Database for PostgreSQL can only be accessed from a private endpoint. This configuration disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.1 ↗
Storage accounts should restrict network access ↗	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow	Audit, Deny, Disabled	1.1.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges		
<a href="#">Storage accounts should restrict network access using virtual network rules ↗</a>	Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.	Audit, Deny, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Storage accounts should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview ↗</a>	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Subnets should be associated with a Network Security Group ↗</a>	Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">VM Image Builder templates should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .	Audit, Disabled, Deny	<a href="#">1.1.0 ↗</a>
<a href="#">Web Application Firewall (WAF) should be</a>	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">enabled for Application Gateway ↗</a>	incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.		

## External Telecommunications Services

ID: FedRAMP High SC-7 (4) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement managed interface for each external service ↗</a>	CMA_C1626 - Implement managed interface for each external service	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement system boundary protection ↗</a>	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Secure the interface to external systems ↗</a>	CMA_0491 - Secure the interface to external systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Prevent Split Tunneling For Remote Devices

ID: FedRAMP High SC-7 (7) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Prevent split tunneling for remote devices ↗</a>	CMA_C1632 - Prevent split tunneling for remote devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Route Traffic To Authenticated Proxy Servers

ID: FedRAMP High SC-7 (8) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Route traffic through authenticated proxy network ↴	CMA_C1633 - Route traffic through authenticated proxy network	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Host-Based Protection

ID: FedRAMP High SC-7 (12) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement system boundary protection ↴	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Isolation Of Security Tools / Mechanisms / Support Components

ID: FedRAMP High SC-7 (13) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Isolate SecurID systems, Security Incident Management systems ↴	CMA_C1636 - Isolate SecurID systems, Security Incident Management systems	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Fail Secure

ID: FedRAMP High SC-7 (18) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage transfers between standby and active system components ↗	CMA_0371 - Manage transfers between standby and active system components	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Dynamic Isolation / Segregation

ID: FedRAMP High SC-7 (20) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure system capable of dynamic isolation of resources ↗	CMA_C1638 - Ensure system capable of dynamic isolation of resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Isolation Of Information System Components

ID: FedRAMP High SC-7 (21) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ boundary protection to isolate information systems ↗	CMA_C1639 - Employ boundary protection to isolate information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Transmission Confidentiality And Integrity

ID: FedRAMP High SC-8 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">App Service apps should only be accessible over HTTPS ↗</a>	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	<a href="#">4.0.0 ↗</a>
<a href="#">App Service apps should require FTPS only ↗</a>	Enable FTPS enforcement for enhanced security.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">App Service apps should use the latest TLS version ↗</a>	Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the latest TLS version for App Service apps to take advantage of security fixes, if any, and/or new functionalities of the latest version.	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Azure HDInsight clusters should use encryption in transit to encrypt communication between Azure HDInsight cluster nodes ↗</a>	Data can be tampered with during transmission between Azure HDInsight cluster nodes. Enabling encryption in transit addresses problems of misuse and tampering during this transmission.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Enforce SSL connection should be enabled for MySQL database servers ↗</a>	Azure Database for MySQL supports connecting your Azure Database for MySQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration enforces that SSL is always enabled for accessing your database server.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Enforce SSL connection should be enabled for PostgreSQL database servers ↗</a>	Azure Database for PostgreSQL supports connecting your Azure Database for PostgreSQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This	Audit, Disabled	<a href="#">1.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	configuration enforces that SSL is always enabled for accessing your database server.		
Function apps should only be accessible over HTTPS ↗	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	5.0.0 ↗
Function apps should require FTPS only ↗	Enable FTPS enforcement for enhanced security.	AuditIfNotExists, Disabled	3.0.0 ↗
Function apps should use the latest TLS version ↗	Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the latest TLS version for Function apps to take advantage of security fixes, if any, and/or new functionalities of the latest version.	AuditIfNotExists, Disabled	2.0.1 ↗
Kubernetes clusters should be accessible only over HTTPS ↗	Use of HTTPS ensures authentication and protects data in transit from network layer eavesdropping attacks. This capability is currently generally available for Kubernetes Service (AKS), and in preview for Azure Arc enabled Kubernetes. For more info, visit <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> ↗	audit, Audit, deny, Deny, disabled, Disabled	8.1.0 ↗
Only secure connections to your Azure Cache for Redis should be enabled ↗	Audit enabling of only connections via SSL to Azure Cache for Redis. Use of secure connections ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking	Audit, Deny, Disabled	1.0.0 ↗
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	1.1.0 ↗
Secure transfer to storage accounts should be enabled ↗	Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication	Audit, Deny, Disabled	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking		
Windows machines should be configured to use secure communication protocols ↴	To protect the privacy of information communicated over the Internet, your machines should use the latest version of the industry-standard cryptographic protocol, Transport Layer Security (TLS). TLS secures communications over a network by encrypting a connection between machines.	AuditIfNotExists, Disabled	4.1.1 ↴

## Cryptographic Or Alternate Physical Protection

ID: FedRAMP High SC-8 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
App Service apps should only be accessible over HTTPS ↴	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	4.0.0 ↴
App Service apps should require FTPS only ↴	Enable FTPS enforcement for enhanced security.	AuditIfNotExists, Disabled	3.0.0 ↴
App Service apps should use the latest TLS version ↴	Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the latest TLS version for App Service apps to take advantage of security fixes, if any, and/or new functionalities of the latest version.	AuditIfNotExists, Disabled	2.0.1 ↴
Azure HDInsight clusters should use encryption in transit to encrypt communication between Azure	Data can be tampered with during transmission between Azure HDInsight cluster nodes. Enabling encryption in transit addresses problems of misuse and tampering during this transmission.	Audit, Deny, Disabled	1.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">HDInsight cluster nodes ↗</a>			
<a href="#">Configure workstations to check for digital certificates ↗</a>	CMA_0073 - Configure workstations to check for digital certificates	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce SSL connection should be enabled for MySQL database servers ↗</a>	Azure Database for MySQL supports connecting your Azure Database for MySQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration enforces that SSL is always enabled for accessing your database server.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Enforce SSL connection should be enabled for PostgreSQL database servers ↗</a>	Azure Database for PostgreSQL supports connecting your Azure Database for PostgreSQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration enforces that SSL is always enabled for accessing your database server.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Function apps should only be accessible over HTTPS ↗</a>	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	<a href="#">5.0.0 ↗</a>
<a href="#">Function apps should require FTPS only ↗</a>	Enable FTPS enforcement for enhanced security.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Function apps should use the latest TLS version ↗</a>	Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the latest TLS version for Function apps to take advantage of security fixes, if	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	any, and/or new functionalities of the latest version.		
Kubernetes clusters should be accessible only over HTTPS ↴	Use of HTTPS ensures authentication and protects data in transit from network layer eavesdropping attacks. This capability is currently generally available for Kubernetes Service (AKS), and in preview for Azure Arc enabled Kubernetes. For more info, visit <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> ↴	audit, Audit, deny, Deny, disabled, Disabled	8.1.0 ↴
Only secure connections to your Azure Cache for Redis should be enabled ↴	Audit enabling of only connections via SSL to Azure Cache for Redis. Use of secure connections ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking	Audit, Deny, Disabled	1.0.0 ↴
Secure transfer to storage accounts should be enabled ↴	Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking	Audit, Deny, Disabled	2.0.0 ↴
Windows machines should be configured to use secure communication protocols ↴	To protect the privacy of information communicated over the Internet, your machines should use the latest version of the industry-standard cryptographic protocol, Transport Layer Security (TLS). TLS secures communications over a network by encrypting a connection between machines.	AuditIfNotExists, Disabled	4.1.1 ↴

## Network Disconnect

ID: FedRAMP High SC-10 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Reauthenticate or terminate a user session ↗	CMA_0421 - Reauthenticate or terminate a user session	Manual, Disabled	1.1.0 ↗

## Cryptographic Key Establishment And Management

ID: FedRAMP High SC-12 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Azure Recovery Services vaults should use customer-managed keys for encrypting backup data ↗	Use customer-managed keys to manage the encryption at rest of your backup data. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/AB-CmkEncryption">https://aka.ms/AB-CmkEncryption</a> ↗.	Audit, Deny, Disabled	1.0.0-preview ↗
[Preview]: IoT Hub device provisioning service data should be encrypted using customer-managed keys (CMK) ↗	Use customer-managed keys to manage the encryption at rest of your IoT Hub device provisioning service. The data is automatically encrypted at rest with service-managed keys, but customer-managed keys (CMK) are commonly required to meet regulatory compliance standards. CMKs enable the data to be encrypted with an Azure Key Vault key created and owned by you. Learn more about CMK encryption at <a href="https://aka.ms/dps/CMK">https://aka.ms/dps/CMK</a> ↗.	Audit, Deny, Disabled	1.0.0-preview ↗
Azure API for FHIR should use a customer-managed key to encrypt data at rest ↗	Use a customer-managed key to control the encryption at rest of the data stored in Azure API for FHIR when this is a regulatory or compliance requirement. Customer-managed keys also deliver double encryption by adding a second layer of encryption on top of the default one done with service-managed keys.	audit, Audit, disabled, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s) (GitHub)	Version
<a href="#">Azure Automation accounts should use customer-managed keys to encrypt data at rest ↗</a>	<p>Use customer-managed keys to manage the encryption at rest of your Azure Automation Accounts. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/automation-cmk">https://aka.ms/automation-cmk</a> ↗.</p>	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Batch account should use customer-managed keys to encrypt data ↗</a>	<p>Use customer-managed keys to manage the encryption at rest of your Batch account's data. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/Batch-CMK">https://aka.ms/Batch-CMK</a> ↗.</p>	Audit, Deny, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Azure Container Instance container group should use customer-managed key for encryption ↗</a>	<p>Secure your containers with greater flexibility using customer-managed keys. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Using customer-managed keys provides additional capabilities to control rotation of the key encryption key or cryptographically erase data.</p>	Audit, Disabled, Deny	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest ↗</a>	<p>Use customer-managed keys to manage the encryption at rest of your Azure Cosmos DB. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle,</p>	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	including rotation and management. Learn more at <a href="https://aka.ms/cosmosdb-cmk">https://aka.ms/cosmosdb-cmk</a> .		
<a href="#">Azure Data Box jobs should use a customer-managed key to encrypt the device unlock password ↗</a>	Use a customer-managed key to control the encryption of the device unlock password for Azure Data Box. Customer-managed keys also help manage access to the device unlock password by the Data Box service in order to prepare the device and copy data in an automated manner. The data on the device itself is already encrypted at rest with Advanced Encryption Standard 256-bit encryption, and the device unlock password is encrypted by default with a Microsoft managed key.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Data Explorer encryption at rest should use a customer-managed key ↗</a>	Enabling encryption at rest using a customer-managed key on your Azure Data Explorer cluster provides additional control over the key being used by the encryption at rest. This feature is oftentimes applicable to customers with special compliance requirements and requires a Key Vault to managing the keys.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure data factories should be encrypted with a customer-managed key ↗</a>	Use customer-managed keys to manage the encryption at rest of your Azure Data Factory. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/adf-cmk">https://aka.ms/adf-cmk</a> .	Audit, Deny, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Azure HDInsight clusters should use customer-managed keys to encrypt data at rest ↗</a>	Use customer-managed keys to manage the encryption at rest of your Azure HDInsight clusters. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key	Audit, Deny, Disabled	<a href="#">1.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/hdi.cmk">https://aka.ms/hdi.cmk</a> .		
Azure HDInsight clusters should use encryption at host to encrypt data at rest <a href="#">🔗</a>	Enabling encryption at host helps protect and safeguard your data to meet your organizational security and compliance commitments. When you enable encryption at host, data stored on the VM host is encrypted at rest and flows encrypted to the Storage service.	Audit, Deny, Disabled	1.0.0 <a href="#">🔗</a>
Azure Machine Learning workspaces should be encrypted with a customer-managed key <a href="#">🔗</a>	Manage encryption at rest of Azure Machine Learning workspace data with customer-managed keys. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/azureml-workspaces-cmk">https://aka.ms/azureml-workspaces-cmk</a> .	Audit, Deny, Disabled	1.0.3 <a href="#">🔗</a>
Azure Monitor Logs clusters should be encrypted with customer-managed key <a href="#">🔗</a>	Create Azure Monitor logs cluster with customer-managed keys encryption. By default, the log data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance. Customer-managed key in Azure Monitor gives you more control over the access to your data, see <a href="https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys">https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys</a> .	audit, Audit, deny, Deny, disabled, Disabled	1.1.0 <a href="#">🔗</a>
Azure Stream Analytics jobs should use customer-managed keys to encrypt data <a href="#">🔗</a>	Use customer-managed keys when you want to securely store any metadata and private data assets of your Stream Analytics jobs in your storage account. This gives you total control over how your Stream Analytics data is encrypted.	audit, Audit, deny, Deny, disabled, Disabled	1.1.0 <a href="#">🔗</a>
Azure Synapse workspaces should use customer-managed keys	Use customer-managed keys to control the encryption at rest of the data stored in Azure Synapse workspaces. Customer-managed keys deliver double encryption by adding a second	Audit, Deny, Disabled	1.0.0 <a href="#">🔗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">to encrypt data at rest ↗</a>	layer of encryption on top of the default encryption with service-managed keys.		
<a href="#">Bot Service should be encrypted with a customer-managed key ↗</a>	Azure Bot Service automatically encrypts your resource to protect your data and meet organizational security and compliance commitments. By default, Microsoft-managed encryption keys are used. For greater flexibility in managing keys or controlling access to your subscription, select customer-managed keys, also known as bring your own key (BYOK).  Learn more about Azure Bot Service encryption: <a href="https://docs.microsoft.com/azure/bot-service/bot-service-encryption">https://docs.microsoft.com/azure/bot-service/bot-service-encryption</a> .	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys ↗</a>	Encrypting OS and data disks using customer-managed keys provides more control and greater flexibility in key management. This is a common requirement in many regulatory and industry compliance standards.	Audit, Deny, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Cognitive Services accounts should enable data encryption with a customer-managed key ↗</a>	Customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data stored in Cognitive Services to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more about customer-managed keys at <a href="https://go.microsoft.com/fwlink/?linkid=2121321">https://go.microsoft.com/fwlink/?linkid=2121321</a> .	Audit, Deny, Disabled	<a href="#">2.1.0 ↗</a>
<a href="#">Container registries should be encrypted with a customer-managed key ↗</a>	Use customer-managed keys to manage the encryption at rest of the contents of your registries. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key	Audit, Deny, Disabled	<a href="#">1.1.2 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/acr/CMK">https://aka.ms/acr/CMK</a> .		
Define a physical key management process <a href="#">↗</a>	CMA_0115 - Define a physical key management process	Manual, Disabled	1.1.0 <a href="#">↗</a>
Define cryptographic use <a href="#">↗</a>	CMA_0120 - Define cryptographic use	Manual, Disabled	1.1.0 <a href="#">↗</a>
Define organizational requirements for cryptographic key management <a href="#">↗</a>	CMA_0123 - Define organizational requirements for cryptographic key management	Manual, Disabled	1.1.0 <a href="#">↗</a>
Determine assertion requirements <a href="#">↗</a>	CMA_0136 - Determine assertion requirements	Manual, Disabled	1.1.0 <a href="#">↗</a>
Event Hub namespaces should use a customer-managed key for encryption <a href="#">↗</a>	Azure Event Hubs supports the option of encrypting data at rest with either Microsoft-managed keys (default) or customer-managed keys. Choosing to encrypt data using customer-managed keys enables you to assign, rotate, disable, and revoke access to the keys that Event Hub will use to encrypt data in your namespace. Note that Event Hub only supports encryption with customer-managed keys for namespaces in dedicated clusters.	Audit, Disabled	1.0.0 <a href="#">↗</a>
HPC Cache accounts should use customer-managed key for encryption <a href="#">↗</a>	Manage encryption at rest of Azure HPC Cache with customer-managed keys. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full	Audit, Disabled, Deny	2.0.0 <a href="#">↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	control and responsibility for the key lifecycle, including rotation and management.		
<a href="#">Issue public key certificates ↗</a>	CMA_0347 - Issue public key certificates	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Logic Apps Integration Service Environment should be encrypted with customer-managed keys ↗</a>	<p>Deploy into Integration Service Environment to manage encryption at rest of Logic Apps data using customer-managed keys. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards.</p> <p>Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management.</p>	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Manage symmetric cryptographic keys ↗</a>	CMA_0367 - Manage symmetric cryptographic keys	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Managed disks should be double encrypted with both platform-managed and customer-managed keys ↗</a>	<p>High security sensitive customers who are concerned of the risk associated with any particular encryption algorithm, implementation, or key being compromised can opt for additional layer of encryption using a different encryption algorithm/mode at the infrastructure layer using platform managed encryption keys. The disk encryption sets are required to use double encryption.</p> <p>Learn more at <a href="https://aka.ms/disks-doubleEncryption">https://aka.ms/disks-doubleEncryption</a>.</p>	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">MySQL servers should use customer-managed keys to encrypt data at rest ↗</a>	<p>Use customer-managed keys to manage the encryption at rest of your MySQL servers. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards.</p> <p>Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management.</p>	AuditIfNotExists, Disabled	<a href="#">1.0.4 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">OS and data disks should be encrypted with a customer-managed key ↗</a>	Use customer-managed keys to manage the encryption at rest of the contents of your managed disks. By default, the data is encrypted at rest with platform-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/disks-cmk">https://aka.ms/disks-cmk</a> ↗.	Audit, Deny, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">PostgreSQL servers should use customer-managed keys to encrypt data at rest ↗</a>	Use customer-managed keys to manage the encryption at rest of your PostgreSQL servers. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management.	AuditIfNotExists, Disabled	<a href="#">1.0.4 ↗</a>
<a href="#">Restrict access to private keys ↗</a>	CMA_0445 - Restrict access to private keys	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Saved-queries in Azure Monitor should be saved in customer storage account for logs encryption ↗</a>	Link storage account to Log Analytics workspace to protect saved-queries with storage account encryption. Customer-managed keys are commonly required to meet regulatory compliance and for more control over the access to your saved-queries in Azure Monitor. For more details on the above, see <a href="https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys?tabs=portal#customer-managed-key-for-saved-queries">https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys?tabs=portal#customer-managed-key-for-saved-queries</a> .	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Service Bus Premium namespaces should use a customer-</a>	Azure Service Bus supports the option of encrypting data at rest with either Microsoft-managed keys (default) or customer-managed keys. Choosing to encrypt data using customer-managed keys enables you to	Audit, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">managed key for encryption ↗</a>	assign, rotate, disable, and revoke access to the keys that Service Bus will use to encrypt data in your namespace. Note that Service Bus only supports encryption with customer-managed keys for premium namespaces.		
<a href="#">SQL managed instances should use customer-managed keys to encrypt data at rest ↗</a>	Implementing Transparent Data Encryption (TDE) with your own key provides you with increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties. This recommendation applies to organizations with a related compliance requirement.	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">SQL servers should use customer-managed keys to encrypt data at rest ↗</a>	Implementing Transparent Data Encryption (TDE) with your own key provides increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties. This recommendation applies to organizations with a related compliance requirement.	Audit, Deny, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Storage account encryption scopes should use customer-managed keys to encrypt data at rest ↗</a>	Use customer-managed keys to manage the encryption at rest of your storage account encryption scopes. Customer-managed keys enable the data to be encrypted with an Azure key-vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more about storage account encryption scopes at <a href="https://aka.ms/encryption-scopes-overview">https://aka.ms/encryption-scopes-overview</a> ↗.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Storage accounts should use customer-managed key for encryption ↗</a>	Secure your blob and file storage account with greater flexibility using customer-managed keys. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Using customer-managed keys provides additional capabilities to control rotation of the key encryption key or cryptographically erase data.	Audit, Disabled	<a href="#">1.0.3 ↗</a>

## Availability

ID: FedRAMP High SC-12 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Maintain availability of information ↗	CMA_C1644 - Maintain availability of information	Manual, Disabled	1.1.0 ↗

## Symmetric Keys

ID: FedRAMP High SC-12 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Produce, control and distribute symmetric cryptographic keys ↗	CMA_C1645 - Produce, control and distribute symmetric cryptographic keys	Manual, Disabled	1.1.0 ↗

## Asymmetric Keys

ID: FedRAMP High SC-12 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Produce, control and distribute asymmetric cryptographic keys ↗	CMA_C1646 - Produce, control and distribute asymmetric cryptographic keys	Manual, Disabled	1.1.0 ↗

## Cryptographic Protection

ID: FedRAMP High SC-13 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define cryptographic use ↗</a>	CMA_0120 - Define cryptographic use	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Collaborative Computing Devices

ID: FedRAMP High SC-15 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Explicitly notify use of collaborative computing devices ↗</a>	CMA_C1649 - Explicitly notify use of collaborative computing devices	Manual, Disabled	<a href="#">1.1.1 ↗</a>
<a href="#">Prohibit remote activation of collaborative computing devices ↗</a>	CMA_C1648 - Prohibit remote activation of collaborative computing devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Public Key Infrastructure Certificates

ID: FedRAMP High SC-17 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Issue public key certificates ↗</a>	CMA_0347 - Issue public key certificates	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Mobile Code

ID: FedRAMP High SC-18 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authorize, monitor, and control usage of mobile code</a>	CMA_C1653 - Authorize, monitor, and control usage of mobile code	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
technologies ↗	technologies		
Define acceptable and unacceptable mobile code technologies ↗	CMA_C1651 - Define acceptable and unacceptable mobile code technologies	Manual, Disabled	1.1.0 ↗
Establish usage restrictions for mobile code technologies ↗	CMA_C1652 - Establish usage restrictions for mobile code technologies	Manual, Disabled	1.1.0 ↗

## Voice Over Internet Protocol

ID: FedRAMP High SC-19 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize, monitor, and control voip ↗	CMA_0025 - Authorize, monitor, and control voip	Manual, Disabled	1.1.0 ↗
Establish voip usage restrictions ↗	CMA_0280 - Establish voip usage restrictions	Manual, Disabled	1.1.0 ↗

## Secure Name / Address Resolution Service (Authoritative Source)

ID: FedRAMP High SC-20 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement a fault tolerant name/address service ↗	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	1.1.0 ↗
Provide secure name and address resolution services ↗	CMA_0416 - Provide secure name and address resolution services	Manual, Disabled	1.1.0 ↗

# Secure Name / Address Resolution Service (Recursive Or Caching Resolver)

ID: FedRAMP High SC-21 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement a fault tolerant name/address service ↗</a>	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Verify software, firmware and information integrity ↗</a>	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Architecture And Provisioning For Name / Address Resolution Service

ID: FedRAMP High SC-22 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement a fault tolerant name/address service ↗</a>	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Session Authenticity

ID: FedRAMP High SC-23 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Configure workstations to check for digital certificates ↗</a>	CMA_0073 - Configure workstations to check for digital certificates	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce random unique session identifiers ↗</a>	CMA_0247 - Enforce random unique session identifiers	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Invalidate Session Identifiers At Logout

ID: FedRAMP High SC-23 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Invalidate session identifiers at logout ↗</a>	CMA_C1661 - Invalidate session identifiers at logout	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Fail In Known State

ID: FedRAMP High SC-24 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Ensure information system fails in known state ↗</a>	CMA_C1662 - Ensure information system fails in known state	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Protection Of Information At Rest

ID: FedRAMP High SC-28 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">App Service Environment should have internal encryption enabled ↗</a>	Setting InternalEncryption to true encrypts the pagefile, worker disks, and internal network traffic between the front ends and workers in an App Service Environment. To learn more, refer to <a href="https://docs.microsoft.com/azure/app-service/environment/app-service-app-service-environment-custom-settings#enable-internal-encryption">https://docs.microsoft.com/azure/app-service/environment/app-service-app-service-environment-custom-settings#enable-internal-encryption</a> .	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Automation account variables should be</a>	It is important to enable encryption of Automation account variable assets when	Audit, Deny, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
encrypted ↴	storing sensitive data		
Azure Data Box jobs should enable double encryption for data at rest on the device ↴	Enable a second layer of software-based encryption for data at rest on the device. The device is already protected via Advanced Encryption Standard 256-bit encryption for data at rest. This option adds a second layer of data encryption.	Audit, Deny, Disabled	1.0.0 ↴
Azure Monitor Logs clusters should be created with infrastructure-encryption enabled (double encryption) ↴	To ensure secure data encryption is enabled at the service level and the infrastructure level with two different encryption algorithms and two different keys, use an Azure Monitor dedicated cluster. This option is enabled by default when supported at the region, see <a href="https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys#customer-managed-key-overview">https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys#customer-managed-key-overview</a> .	audit, Audit, deny, Deny, disabled, Disabled	1.1.0 ↴
Azure Stack Edge devices should use double-encryption ↴	To secure the data at rest on the device, ensure it's double-encrypted, the access to data is controlled, and once the device is deactivated, the data is securely erased off the data disks. Double encryption is the use of two layers of encryption: BitLocker XTS-AES 256-bit encryption on the data volumes and built-in encryption of the hard drives. Learn more in the security overview documentation for the specific Stack Edge device.	audit, Audit, deny, Deny, disabled, Disabled	1.1.0 ↴
Disk encryption should be enabled on Azure Data Explorer ↴	Enabling disk encryption helps protect and safeguard your data to meet your organizational security and compliance commitments.	Audit, Deny, Disabled	2.0.0 ↴
Double encryption should be enabled on Azure Data Explorer ↴	Enabling double encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. When double encryption has been enabled, data in the storage account is encrypted twice, once at the service level and once at the infrastructure level, using two different encryption algorithms and two different keys.	Audit, Deny, Disabled	2.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish a data leakage management procedure ↗	CMA_0255 - Establish a data leakage management procedure	Manual, Disabled	1.1.0 ↗
Infrastructure encryption should be enabled for Azure Database for MySQL servers ↗	Enable infrastructure encryption for Azure Database for MySQL servers to have higher level of assurance that the data is secure. When infrastructure encryption is enabled, the data at rest is encrypted twice using FIPS 140-2 compliant Microsoft managed keys.	Audit, Deny, Disabled	1.0.0 ↗
Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers ↗	Enable infrastructure encryption for Azure Database for PostgreSQL servers to have higher level of assurance that the data is secure. When infrastructure encryption is enabled, the data at rest is encrypted twice using FIPS 140-2 compliant Microsoft managed keys	Audit, Deny, Disabled	1.0.0 ↗
Protect special information ↗	CMA_0409 - Protect special information	Manual, Disabled	1.1.0 ↗
Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign ↗	Service Fabric provides three levels of protection (None, Sign and EncryptAndSign) for node-to-node communication using a primary cluster certificate. Set the protection level to ensure that all node-to-node messages are encrypted and digitally signed	Audit, Deny, Disabled	1.1.0 ↗
Storage accounts should have infrastructure encryption ↗	Enable infrastructure encryption for higher level of assurance that the data is secure. When infrastructure encryption is enabled, data in a storage account is encrypted twice.	Audit, Deny, Disabled	1.0.0 ↗
Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host ↗	To enhance data security, the data stored on the virtual machine (VM) host of your Azure Kubernetes Service nodes VMs should be encrypted at rest. This is a common requirement in many regulatory and industry compliance standards.	Audit, Deny, Disabled	1.0.1 ↗
Transparent Data Encryption on SQL	Transparent data encryption should be enabled to protect data-at-rest and meet compliance requirements	AuditIfNotExists, Disabled	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">databases should be enabled ↗</a>			
<a href="#">Virtual machines and virtual machine scale sets should have encryption at host enabled ↗</a>	<p>Use encryption at host to get end-to-end encryption for your virtual machine and virtual machine scale set data. Encryption at host enables encryption at rest for your temporary disk and OS/data disk caches.</p> <p>Temporary and ephemeral OS disks are encrypted with platform-managed keys when encryption at host is enabled.</p> <p>OS/data disk caches are encrypted at rest with either customer-managed or platform-managed key, depending on the encryption type selected on the disk. Learn more at <a href="https://aka.ms/vm-hbe">https://aka.ms/vm-hbe</a>.</p>	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources ↗</a>	<p>By default, a virtual machine's OS and data disks are encrypted-at-rest using platform-managed keys. Temp disks, data caches and data flowing between compute and storage aren't encrypted. Disregard this recommendation if: 1. using encryption-at-host, or 2. server-side encryption on Managed Disks meets your security requirements. Learn more in: Server-side encryption of Azure Disk Storage: <a href="https://aka.ms/disksse">https://aka.ms/disksse</a>, ↗ Different disk encryption offerings: <a href="https://aka.ms/diskencryptioncomparison">https://aka.ms/diskencryptioncomparison</a></p>	AuditIfNotExists, Disabled	<a href="#">2.0.3 ↗</a>

## Cryptographic Protection

ID: FedRAMP High SC-28 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">App Service Environment should have internal encryption enabled ↗</a>	Setting InternalEncryption to true encrypts the pagefile, worker disks, and internal network traffic between the front ends and workers in an App Service Environment. To learn more, refer to	Audit, Disabled	<a href="#">1.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<a href="https://docs.microsoft.com/azure/app-service/environment/app-service-app-service-environment-custom-settings#enable-internal-encryption">https://docs.microsoft.com/azure/app-service/environment/app-service-app-service-environment-custom-settings#enable-internal-encryption.</a>		
<a href="#">Automation account variables should be encrypted ↗</a>	It is important to enable encryption of Automation account variable assets when storing sensitive data	Audit, Deny, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Azure Data Box jobs should enable double encryption for data at rest on the device ↗</a>	Enable a second layer of software-based encryption for data at rest on the device. The device is already protected via Advanced Encryption Standard 256-bit encryption for data at rest. This option adds a second layer of data encryption.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Monitor Logs clusters should be created with infrastructure-encryption enabled (double encryption) ↗</a>	To ensure secure data encryption is enabled at the service level and the infrastructure level with two different encryption algorithms and two different keys, use an Azure Monitor dedicated cluster. This option is enabled by default when supported at the region, see <a href="https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys#customer-managed-key-overview">https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys#customer-managed-key-overview</a> .	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Azure Stack Edge devices should use double-encryption ↗</a>	To secure the data at rest on the device, ensure it's double-encrypted, the access to data is controlled, and once the device is deactivated, the data is securely erased off the data disks. Double encryption is the use of two layers of encryption: BitLocker XTS-AES 256-bit encryption on the data volumes and built-in encryption of the hard drives. Learn more in the security overview documentation for the specific Stack Edge device.	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Disk encryption should be enabled on Azure Data Explorer ↗</a>	Enabling disk encryption helps protect and safeguard your data to meet your organizational security and compliance commitments.	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Double encryption should be enabled on Azure Data Explorer ↗</a>	Enabling double encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. When double encryption has	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	been enabled, data in the storage account is encrypted twice, once at the service level and once at the infrastructure level, using two different encryption algorithms and two different keys.		
<a href="#">Implement controls to secure all media ↴</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↴
<a href="#">Infrastructure encryption should be enabled for Azure Database for MySQL servers ↴</a>	Enable infrastructure encryption for Azure Database for MySQL servers to have higher level of assurance that the data is secure. When infrastructure encryption is enabled, the data at rest is encrypted twice using FIPS 140-2 compliant Microsoft managed keys.	Audit, Deny, Disabled	1.0.0 ↴
<a href="#">Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers ↴</a>	Enable infrastructure encryption for Azure Database for PostgreSQL servers to have higher level of assurance that the data is secure. When infrastructure encryption is enabled, the data at rest is encrypted twice using FIPS 140-2 compliant Microsoft managed keys	Audit, Deny, Disabled	1.0.0 ↴
<a href="#">Protect data in transit using encryption ↴</a>	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↴
<a href="#">Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign ↴</a>	Service Fabric provides three levels of protection (None, Sign and EncryptAndSign) for node-to-node communication using a primary cluster certificate. Set the protection level to ensure that all node-to-node messages are encrypted and digitally signed	Audit, Deny, Disabled	1.1.0 ↴
<a href="#">Storage accounts should have infrastructure encryption ↴</a>	Enable infrastructure encryption for higher level of assurance that the data is secure. When infrastructure encryption is enabled, data in a storage account is encrypted twice.	Audit, Deny, Disabled	1.0.0 ↴
<a href="#">Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host ↴</a>	To enhance data security, the data stored on the virtual machine (VM) host of your Azure Kubernetes Service nodes VMs should be encrypted at rest. This is a common requirement in many regulatory and industry compliance standards.	Audit, Deny, Disabled	1.0.1 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Transparent Data Encryption on SQL databases should be enabled ↗</a>	Transparent data encryption should be enabled to protect data-at-rest and meet compliance requirements	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Virtual machines and virtual machine scale sets should have encryption at host enabled ↗</a>	Use encryption at host to get end-to-end encryption for your virtual machine and virtual machine scale set data. Encryption at host enables encryption at rest for your temporary disk and OS/data disk caches. Temporary and ephemeral OS disks are encrypted with platform-managed keys when encryption at host is enabled. OS/data disk caches are encrypted at rest with either customer-managed or platform-managed key, depending on the encryption type selected on the disk. Learn more at <a href="https://aka.ms/vm-hbe">https://aka.ms/vm-hbe</a> ↗.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources ↗</a>	By default, a virtual machine's OS and data disks are encrypted-at-rest using platform-managed keys. Temp disks, data caches and data flowing between compute and storage aren't encrypted. Disregard this recommendation if: 1. using encryption-at-host, or 2. server-side encryption on Managed Disks meets your security requirements. Learn more in: Server-side encryption of Azure Disk Storage: <a href="https://aka.ms/disksse">https://aka.ms/disksse</a> , ↗ Different disk encryption offerings: <a href="https://aka.ms/diskencryptioncomparison">https://aka.ms/diskencryptioncomparison</a> ↗	AuditIfNotExists, Disabled	<a href="#">2.0.3 ↗</a>

## Process Isolation

ID: FedRAMP High SC-39 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Maintain separate execution domains for running processes ↗</a>	CMA_C1665 - Maintain separate execution domains for running processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# System And Information Integrity

## System And Information Integrity Policy And Procedures

ID: FedRAMP High SI-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update information integrity policies and procedures ↗</a>	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Flaw Remediation

ID: FedRAMP High SI-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">A vulnerability assessment solution should be enabled on your virtual machines ↗</a>	Audits virtual machines to detect whether they are running a supported vulnerability assessment solution. A core component of every cyber risk and security program is the identification and analysis of vulnerabilities. Azure Security Center's standard pricing tier includes vulnerability scanning for your virtual machines at no extra cost. Additionally, Security Center can automatically deploy this tool for you.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">App Service apps should use latest 'HTTP Version' ↗</a>	Periodically, newer versions are released for HTTP either due to security flaws or to include additional functionality. Using the latest HTTP version for web apps to take advantage of security fixes, if any, and/or new functionalities of the newer version.	AuditIfNotExists, Disabled	<a href="#">4.0.0 ↗</a>
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for Azure SQL Database servers should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for DNS should be enabled ↗	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for Key Vault should be enabled ↗	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Resource Manager should be enabled ↗	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for SQL servers on	Azure Defender for SQL provides functionality for surfacing and mitigating potential	AuditIfNotExists, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">machines should be enabled ↗</a>	database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.		
<a href="#">Function apps should use latest 'HTTP Version' ↗</a>	Periodically, newer versions are released for HTTP either due to security flaws or to include additional functionality. Using the latest HTTP version for web apps to take advantage of security fixes, if any, and/or new functionalities of the newer version.	AuditIfNotExists, Disabled	<a href="#">4.0.0 ↗</a>
<a href="#">Incorporate flaw remediation into configuration management ↗</a>	CMA_C1671 - Incorporate flaw remediation into configuration management	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version ↗</a>	Upgrade your Kubernetes service cluster to a later Kubernetes version to protect against known vulnerabilities in your current Kubernetes version. Vulnerability CVE-2019-9946 has been patched in Kubernetes versions 1.11.9+, 1.12.7+, 1.13.5+, and 1.14.0+	Audit, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Microsoft Defender for Containers should be enabled ↗</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">SQL databases should have vulnerability findings resolved ↗</a>	Monitor vulnerability assessment scan results and recommendations for how to remediate database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">4.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
System updates on virtual machine scale sets should be installed ↴	Audit whether there are any missing system security updates and critical updates that should be installed to ensure that your Windows and Linux virtual machine scale sets are secure.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
System updates should be installed on your machines ↴	Missing security system updates on your servers will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">4.0.0 ↗</a>
Vulnerabilities in security configuration on your machines should be remediated ↴	Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
Vulnerabilities in security configuration on your virtual machine scale sets should be remediated ↴	Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Automated Flaw Remediation Status

ID: FedRAMP High SI-2 (2) Ownership: Shared

[\[ \] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate flaw remediation ↴	CMA_0027 - Automate flaw remediation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Remediate information system flaws ↴	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Time To Remediate Flaws / Benchmarks For Corrective Actions

ID: FedRAMP High SI-2 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish benchmarks for flaw remediation ↗</a>	CMA_C1675 - Establish benchmarks for flaw remediation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Measure the time between flaw identification and flaw remediation ↗</a>	CMA_C1674 - Measure the time between flaw identification and flaw remediation	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Malicious Code Protection

ID: FedRAMP High SI-3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Azure Defender for servers should be enabled ↗</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Block untrusted and unsigned processes that run from USB ↗</a>	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Endpoint protection solution should be installed on virtual machine scale sets ↗</a>	Audit the existence and health of an endpoint protection solution on your virtual machines scale sets, to protect them from threats and vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Manage gateways ↗</a>	CMA_0363 - Manage gateways	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Monitor missing Endpoint Protection in Azure Security Center ↗</a>	Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform a trend analysis on threats ↴	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↴
Perform vulnerability scans ↴	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↴
Review malware detections report weekly ↴	CMA_0475 - Review malware detections report weekly	Manual, Disabled	1.1.0 ↴
Review threat protection status weekly ↴	CMA_0479 - Review threat protection status weekly	Manual, Disabled	1.1.0 ↴
Update antivirus definitions ↴	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↴
Windows Defender Exploit Guard should be enabled on your machines ↴	Windows Defender Exploit Guard uses the Azure Policy Guest Configuration agent. Exploit Guard has four components that are designed to lock down devices against a wide variety of attack vectors and block behaviors commonly used in malware attacks while enabling enterprises to balance their security risk and productivity requirements (Windows only).	AuditIfNotExists, Disabled	2.0.0 ↴

## Central Management

ID: FedRAMP High SI-3 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for servers should be enabled ↴	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↴
Block untrusted and unsigned processes that run from USB ↴	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Endpoint protection solution should be installed on virtual machine scale sets ↗	Audit the existence and health of an endpoint protection solution on your virtual machines scale sets, to protect them from threats and vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Manage gateways ↗	CMA_0363 - Manage gateways	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor missing Endpoint Protection in Azure Security Center ↗	Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review malware detections report weekly ↗	CMA_0475 - Review malware detections report weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Windows Defender Exploit Guard should be enabled on your machines ↗	Windows Defender Exploit Guard uses the Azure Policy Guest Configuration agent. Exploit Guard has four components that are designed to lock down devices against a wide variety of attack vectors and block behaviors commonly used in malware attacks while enabling enterprises to balance their security risk and productivity requirements (Windows only).	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

## Automatic Updates

ID: FedRAMP High SI-3 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↗
Manage gateways ↗	CMA_0363 - Manage gateways	Manual, Disabled	1.1.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Review malware detections report weekly ↗	CMA_0475 - Review malware detections report weekly	Manual, Disabled	1.1.0 ↗
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗

## Nonsignature-Based Detection

ID: FedRAMP High SI-3 (7) Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↗
Manage gateways ↗	CMA_0363 - Manage gateways	Manual, Disabled	1.1.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Review malware detections report weekly ↗	CMA_0475 - Review malware detections report weekly	Manual, Disabled	1.1.0 ↗
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗

# Information System Monitoring

ID: FedRAMP High SI-4 Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: All Internet traffic should be routed via your deployed Azure Firewall ↗	Azure Security Center has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall	AuditIfNotExists, Disabled	3.0.0-preview ↗
[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .	AuditIfNotExists, Disabled	6.0.0-preview ↗
[Preview]: Log Analytics extension should be installed on your Linux Azure Arc machines ↗	This policy audits Linux Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1-preview ↗
[Preview]: Log Analytics extension should be installed on your Windows Azure Arc machines ↗	This policy audits Windows Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1-preview ↗
[Preview]: Network traffic data collection agent should	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic	AuditIfNotExists, Disabled	1.0.2-preview ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">be installed on Linux virtual machines ↗</a>	visualization on the network map, network hardening recommendations and specific network threats.		
<a href="#">[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗</a>	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	<a href="#">1.0.2-preview ↗</a>
<a href="#">Auto provisioning of the Log Analytics agent should be enabled on your subscription ↗</a>	To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for Key Vault should be enabled ↴	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>
Azure Defender for Resource Manager should be enabled ↴	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Azure Defender for servers should be enabled ↴	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>
Azure Defender for SQL servers on machines should be enabled ↴	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↴	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↴</a>
Azure Defender for SQL should be enabled for unprotected	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">SQL Managed Instances ↗</a>			
<a href="#">Guest Configuration extension should be installed on your machines ↗</a>	To ensure secure configurations of in-guest settings of your machine, install the Guest Configuration extension. In-guest settings that the extension monitors include the configuration of the operating system, application configuration or presence, and environment settings. Once installed, in-guest policies will be available such as 'Windows Exploit guard should be enabled'. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Log Analytics agent should be installed on your virtual machine for Azure Security Center monitoring ↗</a>	This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring ↗</a>	Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Containers should be enabled ↗</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	pricing structure (per storage account) for control over coverage and costs.		
Network Watcher should be enabled ↗	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	3.0.0 ↗
Obtain legal opinion for monitoring system activities ↗	CMA_C1688 - Obtain legal opinion for monitoring system activities	Manual, Disabled	1.1.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Provide monitoring information as needed ↗	CMA_C1689 - Provide monitoring information as needed	Manual, Disabled	1.1.0 ↗
Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity ↗	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗	AuditIfNotExists, Disabled	1.0.1 ↗

## Automated Tools For Real-Time Analysis

ID: FedRAMP High SI-4 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Document security operations ↗</a>	CMA_0202 - Document security operations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Turn on sensors for endpoint security solution ↗</a>	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Inbound And Outbound Communications Traffic

ID: FedRAMP High SI-4 (4) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authorize, monitor, and control voip ↗</a>	CMA_0025 - Authorize, monitor, and control voip	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement system boundary protection ↗</a>	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage gateways ↗</a>	CMA_0363 - Manage gateways	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Route traffic through managed network access points ↗</a>	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## System-Generated Alerts

ID: FedRAMP High SI-4 (5) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Alert personnel of information spillage ↗</a>	CMA_0007 - Alert personnel of information spillage	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop an incident response plan ↗</a>	CMA_0145 - Develop an incident response plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Set automated notifications for new and trending cloud applications in your organization ↗	CMA_0495 - Set automated notifications for new and trending cloud applications in your organization	Manual, Disabled	1.1.0 ↗

## Wireless Intrusion Detection

ID: FedRAMP High SI-4 (14) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document wireless access security controls ↗	CMA_C1695 - Document wireless access security controls	Manual, Disabled	1.1.0 ↗

## Unauthorized Network Services

ID: FedRAMP High SI-4 (22) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Detect network services that have not been authorized or approved ↗	CMA_C1700 - Detect network services that have not been authorized or approved	Manual, Disabled	1.1.0 ↗

## Indicators Of Compromise

ID: FedRAMP High SI-4 (24) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Discover any indicators of compromise ↗	CMA_C1702 - Discover any indicators of compromise	Manual, Disabled	1.1.0 ↗

# Security Alerts, Advisories, And Directives

ID: FedRAMP High SI-5 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Disseminate security alerts to personnel ↗	CMA_C1705 - Disseminate security alerts to personnel	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a threat intelligence program ↗	CMA_0260 - Establish a threat intelligence program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Generate internal security alerts ↗	CMA_C1704 - Generate internal security alerts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement security directives ↗	CMA_C1706 - Implement security directives	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Automated Alerts And Advisories

ID: FedRAMP High SI-5 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Use automated mechanisms for security alerts ↗	CMA_C1707 - Use automated mechanisms for security alerts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Security Function Verification

ID: FedRAMP High SI-6 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Create alternative actions for identified anomalies ↗	CMA_C1711 - Create alternative actions for identified anomalies	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Notify personnel of any failed security verification tests ↗	CMA_C1710 - Notify personnel of any failed security verification tests	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform security function verification at a defined frequency ↗	CMA_C1709 - Perform security function verification at a defined frequency	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify security functions ↗	CMA_C1708 - Verify security functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Software, Firmware, And Information Integrity

ID: FedRAMP High SI-7 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Integrity Checks

ID: FedRAMP High SI-7 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Response To Integrity Violations

ID: FedRAMP High SI-7 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ automatic shutdown/restart when violations are detected ↗</a>	CMA_C1715 - Employ automatic shutdown/restart when violations are detected	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Binary Or Machine Executable Code

ID: FedRAMP High SI-7 (14) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Prohibit binary/machine-executable code ↗</a>	CMA_C1717 - Prohibit binary/machine-executable code	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information Input Validation

ID: FedRAMP High SI-10 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Perform information input validation ↗</a>	CMA_C1723 - Perform information input validation	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Error Handling

ID: FedRAMP High SI-11 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Generate error messages ↗</a>	CMA_C1724 - Generate error messages	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Reveal error messages ↗</a>	CMA_C1725 - Reveal error messages	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information Handling And Retention

ID: FedRAMP High SI-12 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage the input, output, processing, and storage of data ↗</a>	CMA_0369 - Manage the input, output, processing, and storage of data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review label activity and analytics ↗</a>	CMA_0474 - Review label activity and analytics	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Memory Protection

ID: FedRAMP High SI-16 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Azure Defender for servers should be enabled ↗</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Windows Defender Exploit Guard should be enabled on your machines ↗</a>	Windows Defender Exploit Guard uses the Azure Policy Guest Configuration agent. Exploit Guard has four components that are designed to lock down devices against a wide variety of attack vectors and block behaviors commonly used in malware attacks while enabling	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
enterprises to balance their security risk and productivity requirements (Windows only).			

## Next steps

Additional articles about Azure Policy:

- [Regulatory Compliance](#) overview.
- See the [initiative definition structure](#).
- Review other examples at [Azure Policy samples](#).
- Review [Understanding policy effects](#).
- Learn how to [remediate non-compliant resources](#).

# Details of the FedRAMP Moderate Regulatory Compliance built-in initiative

Article • 01/02/2024

The following article details how the Azure Policy Regulatory Compliance built-in initiative definition maps to **compliance domains** and **controls** in FedRAMP Moderate. For more information about this compliance standard, see [FedRAMP Moderate](#). To understand *Ownership*, see [Azure Policy policy definition](#) and [Shared responsibility in the cloud](#).

The following mappings are to the **FedRAMP Moderate** controls. Many of the controls are implemented with an [Azure Policy](#) initiative definition. To review the complete initiative definition, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **FedRAMP Moderate** Regulatory Compliance built-in initiative definition.

## Important

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policy definitions themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between compliance domains, controls, and Azure Policy definitions for this compliance standard may change over time. To view the change history, see the [GitHub Commit History](#).

## Access Control

### Access Control Policy And Procedures

ID: FedRAMP Moderate AC-1 Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review access control policies and procedures ↗	CMA_0457 - Review access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Account Management

ID: FedRAMP Moderate AC-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
A maximum of 3 owners should be designated for your subscription ↗	It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
An Azure Active Directory administrator should be provisioned for SQL servers ↗	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
App Service apps should use managed identity ↗	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Assign account managers ↗	CMA_0015 - Assign account managers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Audit usage of custom RBAC roles ↗	Audit built-in roles such as 'Owner, Contributer, Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and	Audit, Disabled	<a href="#">1.0.1 ↗</a>

<b>Name</b>  (Azure portal)	<b>Description</b>	<b>Effect(s)</b>	<b>Version</b>  (GitHub)
	requires a rigorous review and threat modeling		
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	1.1.0 ↗
<a href="#">Blocked accounts with owner permissions on Azure resources should be removed ↗</a>	Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in.	AuditIfExists, Disabled	1.0.0 ↗
<a href="#">Blocked accounts with read and write permissions on Azure resources should be removed ↗</a>	Deprecated accounts should be removed from your subscriptions. Deprecated accounts are accounts that have been blocked from signing in.	AuditIfExists, Disabled	1.0.0 ↗
<a href="#">Cognitive Services accounts should have local authentication methods disabled ↗</a>	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
<a href="#">Define and enforce conditions for shared and group accounts ↗</a>	CMA_0117 - Define and enforce conditions for shared and group accounts	Manual, Disabled	1.1.0 ↗
<a href="#">Define information system account types ↗</a>	CMA_0121 - Define information system account types	Manual, Disabled	1.1.0 ↗
<a href="#">Document access privileges ↗</a>	CMA_0186 - Document access privileges	Manual, Disabled	1.1.0 ↗
<a href="#">Establish conditions for role membership ↗</a>	CMA_0269 - Establish conditions for role membership	Manual, Disabled	1.1.0 ↗
<a href="#">Function apps should use managed identity ↗</a>	Use a managed identity for enhanced authentication security	AuditIfExists, Disabled	3.0.0 ↗
<a href="#">Guest accounts with owner permissions on Azure resources should be removed ↗</a>	External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.	AuditIfExists, Disabled	1.0.0 ↗
<a href="#">Guest accounts with read permissions on</a>	External accounts with read privileges should be removed from your subscription in order to prevent unmonitored access.	AuditIfExists, Disabled	1.0.0 ↗

Azure resources Name <a href="#">should be removed ↴</a> (Azure portal)	Description	Effect(s)	Version (GitHub)
Guest accounts with write permissions on Azure resources should be removed ↴	External accounts with write privileges should be removed from your subscription in order to prevent unmonitored access.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Monitor account activity ↴	CMA_0377 - Monitor account activity	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Notify Account Managers of customer controlled accounts ↴	CMA_C1009 - Notify Account Managers of customer controlled accounts	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Reissue authenticators for changed groups and accounts ↴	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Require approval for account creation ↴	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Restrict access to privileged accounts ↴	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review account provisioning logs ↴	CMA_0460 - Review account provisioning logs	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review user accounts ↴	CMA_0480 - Review user accounts	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Service Fabric clusters should only use Azure Active Directory for client authentication ↴	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	<a href="#">1.1.0 ↴</a>

## Automated System Account Management

ID: FedRAMP Moderate AC-2 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An Azure Active Directory	Audit provisioning of an Azure Active Directory administrator for your SQL server	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
administrator should be provisioned for SQL servers ↗	to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services		
Automate account management ↗	CMA_0026 - Automate account management	Manual, Disabled	1.1.0 ↗
Cognitive Services accounts should have local authentication methods disabled ↗	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> .	Audit, Deny, Disabled	1.0.0 ↗
Manage system and admin accounts ↗	CMA_0368 - Manage system and admin accounts	Manual, Disabled	1.1.0 ↗
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	1.1.0 ↗
Notify when account is not needed ↗	CMA_0383 - Notify when account is not needed	Manual, Disabled	1.1.0 ↗
Service Fabric clusters should only use Azure Active Directory for client authentication ↗	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	1.1.0 ↗

## Disable Inactive Accounts

ID: FedRAMP Moderate AC-2 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	1.1.0 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗

## Automated Audit Actions

ID: FedRAMP Moderate AC-2 (4) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate account management ↗</a>	CMA_0026 - Automate account management	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage system and admin accounts ↗</a>	CMA_0368 - Manage system and admin accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Monitor access across the organization ↗</a>	CMA_0376 - Monitor access across the organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Notify when account is not needed ↗</a>	CMA_0383 - Notify when account is not needed	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Inactivity Logout

ID: FedRAMP Moderate AC-2 (5) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define and enforce inactivity log policy ↗</a>	CMA_C1017 - Define and enforce inactivity log policy	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Role-Based Schemes

ID: FedRAMP Moderate AC-2 (7) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An Azure Active Directory administrator should be provisioned for SQL servers ↗	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	1.0.0 ↗
Audit privileged functions ↗	CMA_0019 - Audit privileged functions	Manual, Disabled	1.1.0 ↗
Audit usage of custom RBAC roles ↗	Audit built-in roles such as 'Owner', 'Contributer', 'Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling	Audit, Disabled	1.0.1 ↗
Cognitive Services accounts should have local authentication methods disabled ↗	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
Monitor account activity ↗	CMA_0377 - Monitor account activity	Manual, Disabled	1.1.0 ↗
Monitor privileged role assignment ↗	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	1.1.0 ↗
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	1.1.0 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗
Service Fabric clusters should only use Azure Active Directory for client authentication ↗	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	1.1.0 ↗
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↗

## Restrictions On Use Of Shared Groups / Accounts

ID: FedRAMP Moderate AC-2 (9) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define and enforce conditions for shared and group accounts ↗	CMA_0117 - Define and enforce conditions for shared and group accounts	Manual, Disabled	1.1.0 ↗

## Shared / Group Account Credential Termination

ID: FedRAMP Moderate AC-2 (10) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Terminate customer controlled account credentials ↗	CMA_C1022 - Terminate customer controlled account credentials	Manual, Disabled	1.1.0 ↗

## Account Monitoring / Atypical Usage

ID: FedRAMP Moderate AC-2 (12) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .	AuditIfNotExists, Disabled	6.0.0-preview ↗
Azure Defender for	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure	AuditIfNotExists, Disabled	1.0.3 ↗

App Service Name should be (Azure portal) enabled ↗	Description	Effect(s)	Version (GitHub)
Azure Defender for Azure SQL Database servers should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for DNS should be enabled ↗	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for Key Vault should be enabled ↗	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Resource Manager should be enabled ↗	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for SQL servers on machines	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities	AuditIfNotExists, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
should be enabled ↗	that could indicate threats to SQL databases, and discovering and classifying sensitive data.		
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↗
Management ports of virtual machines should be protected with just-in-time network access control ↗	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.0.0 ↗
Microsoft Defender for Containers should be enabled ↗	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	1.0.0 ↗
Microsoft Defender for Storage should be enabled ↗	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	1.0.0 ↗
Monitor account activity ↗	CMA_0377 - Monitor account activity	Manual, Disabled	1.1.0 ↗
Report atypical behavior of user accounts ↗	CMA_C1025 - Report atypical behavior of user accounts	Manual, Disabled	1.1.0 ↗

# Access Enforcement

ID: FedRAMP Moderate AC-3 Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accounts with owner permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Accounts with read permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Accounts with write permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗ .	modify	<a href="#">4.0.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy	modify	<a href="#">4.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .		
An Azure Active Directory administrator should be provisioned for SQL servers ↴	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
App Service apps should use managed identity ↴	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>
Audit Linux machines that have accounts without passwords ↴	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Linux machines that have accounts without passwords	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>
Authentication to Linux machines should require SSH keys ↴	Although SSH itself provides an encrypted connection, using passwords with SSH still leaves the VM vulnerable to brute-force attacks. The most secure option for authenticating to an Azure Linux virtual machine over SSH is with a public-private key pair, also known as SSH keys. Learn more: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed">https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed</a> .	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↴</a>
Authorize access to security functions and information ↴	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Authorize and manage access ↴	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Cognitive Services accounts should have local authentication methods disabled ↴	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> .	Audit, Deny, Disabled	<a href="#">1.0.0 ↴</a>
Deploy the Linux Guest	This policy deploys the Linux Guest Configuration extension to Linux virtual	deployIfNotExists	<a href="#">3.0.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configuration extension to enable Guest Configuration assignments on Linux VMs ↗	machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.		
Enforce logical access ↗	CMA_0245 - Enforce logical access	Manual, Disabled	<a href="#">1.1.0</a> ↗
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0</a> ↗
Function apps should use managed identity ↗	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0</a> ↗
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0</a> ↗
Review user groups and applications with access to sensitive data ↗	CMA_0481 - Review user groups and applications with access to sensitive data	Manual, Disabled	<a href="#">1.1.0</a> ↗
Service Fabric clusters should only use Azure Active Directory for client authentication ↗	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	<a href="#">1.1.0</a> ↗
Storage accounts should be migrated to new Azure Resource Manager resources ↗	Use new Azure Resource Manager for your storage accounts to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and	Audit, Deny, Disabled	<a href="#">1.0.0</a> ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
	resource groups for easier security management		
Virtual machines should be migrated to new Azure Resource Manager resources ↴	Use new Azure Resource Manager for your virtual machines to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management	Audit, Deny, Disabled	1.0.0 ↴

## Information Flow Enforcement

ID: FedRAMP Moderate AC-4 Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
[Preview]: All Internet traffic should be routed via your deployed Azure Firewall ↴	Azure Security Center has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall		
[Preview]: Storage account public access should be disallowed ↴	Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it.	audit, Audit, deny, Deny, disabled, Disabled	3.1.0- preview ↴
Adaptive network hardening recommendations should be applied	Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface	AuditIfNotExists, Disabled	3.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
on internet facing virtual machines ↗			
All network ports should be restricted on network security groups associated to your virtual machine ↗	Azure Security Center has identified some of your network security groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.	AuditIfNotExists, Disabled	3.0.0 ↗
API Management services should use a virtual network ↗	Azure Virtual Network deployment provides enhanced security, isolation and allows you to place your API Management service in a non-internet routable network that you control access to. These networks can then be connected to your on-premises networks using various VPN technologies, which enables access to your backend services within the network and/or on-premises. The developer portal and API gateway, can be configured to be accessible either from the Internet or only within the virtual network.	Audit, Deny, Disabled	1.0.2 ↗
App Configuration should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> ↗ .	AuditIfNotExists, Disabled	1.0.2 ↗
App Service apps should not have CORS configured to allow every resource to access your apps ↗	Cross-Origin Resource Sharing (CORS) should not allow all domains to access your app. Allow only required domains to interact with your app.	AuditIfNotExists, Disabled	2.0.0 ↗
Authorized IP ranges should be	Restrict access to the Kubernetes Service Management API by granting API access	Audit, Disabled	2.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">defined on Kubernetes Services ↗</a>	only to IP addresses in specific ranges. It is recommended to limit access to authorized IP ranges to ensure that only applications from allowed networks can access the cluster.		
<a href="#">Azure API for FHIR should use private link ↗</a>	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> ↗ .	Audit, Disabled	1.0.0 ↗
<a href="#">Azure Cache for Redis should use private link ↗</a>	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
<a href="#">Azure Cognitive Search service should use a SKU that supports private link ↗</a>	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
<a href="#">Azure Cognitive Search services should disable public network access ↗</a>	Disabling public network access improves security by ensuring that your Azure Cognitive Search service is not exposed on the public internet. Creating private endpoints can limit exposure of your Search service. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
<a href="#">Azure Cognitive Search services</a>	Azure Private Link lets you connect your virtual network to Azure services without a	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should use private link ↗</a>	<p>public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.</p>		
<a href="#">Azure Cosmos DB accounts should have firewall rules ↗</a>	<p>Firewall rules should be defined on your Azure Cosmos DB accounts to prevent traffic from unauthorized sources. Accounts that have at least one IP rule defined with the virtual network filter enabled are deemed compliant. Accounts disabling public access are also deemed compliant.</p>	Audit, Deny, Disabled	<a href="#">2.0.0</a> ↗
<a href="#">Azure Data Factory should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a>.</p>	AuditIfNotExists, Disabled	<a href="#">1.0.0</a> ↗
<a href="#">Azure Event Grid domains should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> ↗.</p>	Audit, Disabled	<a href="#">1.0.2</a> ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Event Grid topics should use private link ↴	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> .	Audit, Disabled	1.0.2 ↴
Azure File Sync should use private link ↴	Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.	AuditIfNotExists, Disabled	1.0.0 ↴
Azure Key Vault should have firewall enabled ↴	Enable the key vault firewall so that the key vault is not accessible by default to any public IPs. Optionally, you can configure specific IP ranges to limit access to those networks. Learn more at: <a href="https://docs.microsoft.com/azure/key-vault/general/network-security">https://docs.microsoft.com/azure/key-vault/general/network-security</a>	Audit, Deny, Disabled	3.2.1 ↴
Azure Key Vaults should use private link ↴	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink</a> .	[parameters('audit_effect')]	1.2.1 ↴
Azure Machine Learning workspaces	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform	Audit, Disabled	1.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should use private link ↗</a>	handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .		
<a href="#">Azure Service Bus namespaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
<a href="#">Azure SignalR Service should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .	Audit, Disabled	1.0.0 ↗
<a href="#">Azure Synapse workspaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a> .	Audit, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Web PubSub Service should use private link ↗	<p>Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks.</p> <p>Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a>.</p>	Audit, Disabled	1.0.0 ↗
Cognitive Services accounts should disable public network access ↗	<p>To improve the security of Cognitive Services accounts, ensure that it isn't exposed to the public internet and can only be accessed from a private endpoint. Disable the public network access property as described in <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a>. This option disables access from any public address space outside the Azure IP range, and denies all logins that match IP or virtual network-based firewall rules. This reduces data leakage risks.</p>	Audit, Deny, Disabled	3.0.1 ↗
Cognitive Services accounts should restrict network access ↗	<p>Network access to Cognitive Services accounts should be restricted. Configure network rules so only applications from allowed networks can access the Cognitive Services account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges.</p>	Audit, Deny, Disabled	3.0.0 ↗
Cognitive Services should use private link ↗	<p>Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage.</p> <p>Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a>.</p>	Audit, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p><a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a>.</p>		
Container registries should not allow unrestricted network access ↗	<p>Azure container registries by default accept connections over the internet from hosts on any network. To protect your registries from potential threats, allow access from only specific private endpoints, public IP addresses or address ranges. If your registry doesn't have network rules configured, it will appear in the unhealthy resources. Learn more about Container Registry network rules here:</p> <p><a href="https://aka.ms/acr/privatelink">https://aka.ms/acr/privatelink</a>, ↗ <a href="https://aka.ms/acr/portal/public-network">https://aka.ms/acr/portal/public-network</a> ↗ and <a href="https://aka.ms/acr/vnet">https://aka.ms/acr/vnet</a> .</p>	Audit, Deny, Disabled	2.0.0 ↗
Container registries should use private link ↗	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a> .</p>	Audit, Disabled	1.0.1 ↗
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	1.1.0 ↗
CosmosDB accounts should use private link ↗	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at:</p> <p><a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a>.</p>	Audit, Disabled	1.0.0 ↗
Disk access resources should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a>.</p>		
<a href="#">Employ flow control mechanisms of encrypted information ↗</a>	CMA_0211 - Employ flow control mechanisms of encrypted information	Manual, Disabled	1.1.0 ↗
<a href="#">Event Hub namespaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a> .	AuditIfExists, Disabled	1.0.0 ↗
<a href="#">Internet-facing virtual machines should be protected with network security groups ↗</a>	Protect your virtual machines from potential threats by restricting access to them with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsg-doc">https://aka.ms/nsg-doc</a>	AuditIfExists, Disabled	3.0.0 ↗
<a href="#">IoT Hub device provisioning service instances should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a> .	Audit, Disabled	1.0.0 ↗
<a href="#">IP Forwarding on your virtual machine should be disabled ↗</a>	Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely	AuditIfExists, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	required (e.g., when using the VM as a network virtual appliance), and therefore, this should be reviewed by the network security team.		
<a href="#">Management ports of virtual machines should be protected with just-in-time network access control ↴</a>	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>
<a href="#">Management ports should be closed on your virtual machines ↴</a>	Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>
<a href="#">Non-internet-facing virtual machines should be protected with network security groups ↴</a>	Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsg-doc">https://aka.ms/nsg-doc</a> ↴	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>
<a href="#">Private endpoint connections on Azure SQL Database should be enabled ↴</a>	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Private endpoint should be enabled for MariaDB servers ↴</a>	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>
<a href="#">Private endpoint should be enabled for MySQL servers ↴</a>	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	all other IP addresses, including within Azure.		
Private endpoint should be enabled for PostgreSQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Public network access on Azure SQL Database should be disabled ↗	Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP or virtual network based firewall rules.	Audit, Deny, Disabled	1.1.0 ↗
Public network access should be disabled for MariaDB servers ↗	Disable the public network access property to improve security and ensure your Azure Database for MariaDB can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↗
Public network access should be disabled for MySQL servers ↗	Disable the public network access property to improve security and ensure your Azure Database for MySQL can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↗
Public network access should be disabled for PostgreSQL servers ↗	Disable the public network access property to improve security and ensure your Azure Database for PostgreSQL can only be accessed from a private endpoint. This configuration disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.1 ↗
Storage accounts should restrict	Network access to storage accounts should be restricted. Configure network rules so	Audit, Deny, Disabled	1.1.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">network access ↗</a>	only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges		
<a href="#">Storage accounts should restrict network access using virtual network rules ↗</a>	Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.	Audit, Deny, Disabled	1.0.1 ↗
<a href="#">Storage accounts should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview</a> ↗	AuditIfNotExists, Disabled	2.0.0 ↗
<a href="#">Subnets should be associated with a Network Security Group ↗</a>	Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.	AuditIfNotExists, Disabled	3.0.0 ↗
<a href="#">VM Image Builder templates should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .	Audit, Disabled, Deny	1.1.0 ↗

# Physical / Logical Separation Of Information Flows

ID: FedRAMP Moderate AC-4 (21) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control information flow ↗</a>	CMA_0079 - Control information flow	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish firewall and router configuration standards ↗</a>	CMA_0272 - Establish firewall and router configuration standards	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish network segmentation for card holder data environment ↗</a>	CMA_0273 - Establish network segmentation for card holder data environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify and manage downstream information exchanges ↗</a>	CMA_0298 - Identify and manage downstream information exchanges	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Separation Of Duties

ID: FedRAMP Moderate AC-5 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define access authorizations to support separation of duties ↗</a>	CMA_0116 - Define access authorizations to support separation of duties	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document separation of duties ↗</a>	CMA_0204 - Document separation of duties	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Separate duties of individuals ↗</a>	CMA_0492 - Separate duties of individuals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">There should be more than one owner assigned to your subscription ↗</a>	It is recommended to designate more than one subscription owner in order to have administrator access redundancy.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

# Least Privilege

ID: FedRAMP Moderate AC-6 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
A maximum of 3 owners should be designated for your subscription ↗	It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Audit usage of custom RBAC roles ↗	Audit built-in roles such as 'Owner, Contributer, Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling	Audit, Disabled	<a href="#">1.0.1 ↗</a>
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Employ least privilege access ↗	CMA_0212 - Employ least privilege access	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Authorize Access To Security Functions

ID: FedRAMP Moderate AC-6 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize access to security functions and information ↗	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Authorize and manage access ↗	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Privileged Accounts

ID: FedRAMP Moderate AC-6 (5) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Restrict access to privileged accounts ↗</a>	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Auditing Use Of Privileged Functions

ID: FedRAMP Moderate AC-6 (9) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit privileged functions ↗</a>	CMA_0019 - Audit privileged functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct a full text analysis of logged privileged commands ↗</a>	CMA_0056 - Conduct a full text analysis of logged privileged commands	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Monitor privileged role assignment ↗</a>	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Restrict access to privileged accounts ↗</a>	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Revoke privileged roles as appropriate ↗</a>	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Use privileged identity management ↗</a>	CMA_0533 - Use privileged identity management	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Unsuccessful Logon Attempts

ID: FedRAMP Moderate AC-7 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Enforce a limit of consecutive failed login attempts ↗</a>	CMA_C1044 - Enforce a limit of consecutive failed login attempts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Concurrent Session Control

ID: FedRAMP Moderate AC-10 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
Define and enforce the limit of concurrent sessions ↗	CMA_C1050 - Define and enforce the limit of concurrent sessions	Manual, Disabled	1.1.0 ↗

## Session Termination

ID: FedRAMP Moderate AC-12 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
Terminate user session automatically ↗	CMA_C1054 - Terminate user session automatically	Manual, Disabled	1.1.0 ↗

## Permitted Actions Without Identification Or Authentication

ID: FedRAMP Moderate AC-14 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
Identify actions allowed without authentication ↗	CMA_0295 - Identify actions allowed without authentication	Manual, Disabled	1.1.0 ↗

## Remote Access

ID: FedRAMP Moderate AC-17 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	4.0.0 ↗
Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	4.0.0 ↗
App Configuration should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> .	AuditIfNotExists, Disabled	1.0.2 ↗
App Service apps should have remote debugging turned off ↗	Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit Linux machines that allow remote connections from accounts without passwords <a href="#">↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Linux machines that allow remote connections from accounts without passwords	AuditIfNotExists, Disabled	3.0.0 <a href="#">↗</a>
Authorize remote access <a href="#">↗</a>	CMA_0024 - Authorize remote access	Manual, Disabled	1.1.0 <a href="#">↗</a>
Azure API for FHIR should use private link <a href="#">↗</a>	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> .	Audit, Disabled	1.0.0 <a href="#">↗</a>
Azure Cache for Redis should use private link <a href="#">↗</a>	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 <a href="#">↗</a>
Azure Cognitive Search service should use a SKU that supports private link <a href="#">↗</a>	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Deny, Disabled	1.0.0 <a href="#">↗</a>
Azure Cognitive	Azure Private Link lets you connect your virtual network to Azure services without a	Audit, Disabled	1.0.0 <a href="#">↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Search services should use private link ↗</a>	<p>public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.</p>		
<a href="#">Azure Data Factory should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a>.</p>	AuditIfNotExists, Disabled	1.0.0 ↗
<a href="#">Azure Event Grid domains should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> ↗.</p>	Audit, Disabled	1.0.2 ↗
<a href="#">Azure Event Grid topics should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn</p>	Audit, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>more at:  <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a>.</p>		
Azure File Sync should use private link <a href="#">♂</a>	Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.	AuditIfNotExists, Disabled	1.0.0 <a href="#">♂</a>
Azure Key Vaults should use private link <a href="#">♂</a>	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink</a> .	[parameters('audit_effect')]	1.2.1 <a href="#">♂</a>
Azure Machine Learning workspaces should use private link <a href="#">♂</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .	Audit, Disabled	1.0.0 <a href="#">♂</a>
Azure Service Bus namespaces should use private link <a href="#">♂</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at:	AuditIfNotExists, Disabled	1.0.0 <a href="#">♂</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .		
Azure SignalR Service should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .	Audit, Disabled	1.0.0 ↗
Azure Spring Cloud should use network injection ↗	Azure Spring Cloud instances should use virtual network injection for the following purposes: 1. Isolate Azure Spring Cloud from Internet. 2. Enable Azure Spring Cloud to interact with systems in either on premises data centers or Azure service in other virtual networks. 3. Empower customers to control inbound and outbound network communications for Azure Spring Cloud.	Audit, Disabled, Deny	1.2.0 ↗
Azure Synapse workspaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a> .	Audit, Disabled	1.0.1 ↗
Azure Web PubSub Service should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks.</p> <p>Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a>.</p>		
Cognitive Services should use private link <a href="#">↗</a>	<p>Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage.</p> <p>Learn more about private links at: <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a>.</p>	Audit, Disabled	3.0.0 <a href="#">↗</a>
Container registries should use private link <a href="#">↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a>.</p>	Audit, Disabled	1.0.1 <a href="#">↗</a>
CosmosDB accounts should use private link <a href="#">↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a>.</p>	Audit, Disabled	1.0.0 <a href="#">↗</a>
Deploy the Linux Guest Configuration	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are	deployIfNotExists	3.0.0 <a href="#">↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">extension to enable Guest Configuration assignments on Linux VMs</a>	supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .		
<a href="#">Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs</a>	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	<a href="#">1.2.0</a>
<a href="#">Disk access resources should use private link</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.0</a>
<a href="#">Document mobility training</a>	CMA_0191 - Document mobility training	Manual, Disabled	<a href="#">1.1.0</a>
<a href="#">Document remote access guidelines</a>	CMA_0196 - Document remote access guidelines	Manual, Disabled	<a href="#">1.1.0</a>
<a href="#">Event Hub namespaces should use private link</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure	AuditIfNotExists, Disabled	<a href="#">1.0.0</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a> .		
Function apps should have remote debugging turned off ↴	Remote debugging requires inbound ports to be opened on Function apps. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0 ↴
Implement controls to secure alternate work sites ↴	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	1.1.0 ↴
IoT Hub device provisioning service instances should use private link ↴	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a> ↴ .	Audit, Disabled	1.0.0 ↴
Private endpoint connections on Azure SQL Database should be enabled ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↴
Private endpoint should be enabled for MariaDB servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Private endpoint should be enabled for MySQL servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↴
Private endpoint should be enabled for PostgreSQL servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↴
Provide privacy training ↴	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↴
Storage accounts should restrict network access ↴	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges	Audit, Deny, Disabled	1.1.1 ↴
Storage accounts should use private link ↴	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview</a> ↴	AuditIfNotExists, Disabled	2.0.0 ↴
VM Image Builder templates	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform	Audit, Disabled, Deny	1.1.0 ↴

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">should use private link ↗</a>	handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .		

## Automated Monitoring / Control

ID: FedRAMP Moderate AC-17 (1) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	<a href="#">4.0.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	<a href="#">4.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">App Configuration should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> ↗.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">App Service apps should have remote debugging turned off ↗</a>	Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Audit Linux machines that allow remote connections from accounts without passwords ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Linux machines that allow remote connections from accounts without passwords	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Azure API for FHIR should use private link ↗</a>	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> ↗.	Audit, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Cache for Redis should use private link ↗</a>	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Cognitive Search service should use a SKU that supports private link ↗	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.	Audit, Disabled	1.0.0 ↗
Azure Data Factory should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Event Grid domains should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain	Audit, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> .		
Azure Event Grid topics should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> .	Audit, Disabled	1.0.2 ↗
Azure File Sync should use private link ↗	Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Key Vaults should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink</a> .	[parameters('audit_effect')]	1.2.1 ↗
Azure Machine Learning workspaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .		
Azure Service Bus namespaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure SignalR Service should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .	Audit, Disabled	1.0.0 ↗
Azure Spring Cloud should use network injection ↗	Azure Spring Cloud instances should use virtual network injection for the following purposes: 1. Isolate Azure Spring Cloud from Internet. 2. Enable Azure Spring Cloud to interact with systems in either on premises data centers or Azure service in other virtual networks. 3. Empower customers to control inbound and outbound network communications for Azure Spring Cloud.	Audit, Disabled, Deny	1.2.0 ↗
Azure Synapse workspaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the	Audit, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at:  <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a>.</p>		
Azure Web PubSub Service should use private link ↗	<p>Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks.</p> <p>Learn more about private links at:  <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a>.</p>	Audit, Disabled	1.0.0 ↗
Cognitive Services should use private link ↗	<p>Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage.</p> <p>Learn more about private links at:  <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a>.</p>	Audit, Disabled	3.0.0 ↗
Container registries should use private link ↗	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a>.</p>	Audit, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
CosmosDB accounts should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a> .	Audit, Disabled	1.0.0 ↗
Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↗	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	3.0.0 ↗
Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs ↗	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	1.2.0 ↗
Disk access resources should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private	AuditIfExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a> .		
Event Hub namespaces should use private link ↴	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0 ↴
Function apps should have remote debugging turned off ↴	Remote debugging requires inbound ports to be opened on Function apps. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0 ↴
IoT Hub device provisioning service instances should use private link ↴	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a> .	Audit, Disabled	1.0.0 ↴
Monitor access across the organization ↴	CMA_0376 - Monitor access across the organization	Manual, Disabled	1.1.0 ↴
Private endpoint connections on Azure SQL Database should be enabled ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↴
Private endpoint	Private endpoint connections enforce secure communication by enabling private	AuditIfNotExists, Disabled	1.0.2 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should be enabled for MariaDB servers ↗</a>	connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.		
<a href="#">Private endpoint should be enabled for MySQL servers ↗</a>	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
<a href="#">Private endpoint should be enabled for PostgreSQL servers ↗</a>	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
<a href="#">Storage accounts should restrict network access ↗</a>	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges	Audit, Deny, Disabled	1.1.1 ↗
<a href="#">Storage accounts should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview</a> ↗	AuditIfNotExists, Disabled	2.0.0 ↗
<a href="#">VM Image Builder</a>	Azure Private Link lets you connect your virtual network to Azure services without a	Audit, Disabled, Deny	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">templates should use private link ↗</a>	public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .		

## Protection Of Confidentiality / Integrity Using Encryption

ID: FedRAMP Moderate AC-17 (2) Ownership: Shared

[\[ \]](#) Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Notify users of system logon or access ↗</a>	CMA_0382 - Notify users of system logon or access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Protect data in transit using encryption ↗</a>	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Managed Access Control Points

ID: FedRAMP Moderate AC-17 (3) Ownership: Shared

[\[ \]](#) Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Route traffic through managed network access points ↗</a>	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Privileged Commands / Access

ID: FedRAMP Moderate AC-17 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authorize remote access ↗</a>	CMA_0024 - Authorize remote access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Authorize remote access to privileged commands ↗</a>	CMA_C1064 - Authorize remote access to privileged commands	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document remote access guidelines ↗</a>	CMA_0196 - Document remote access guidelines	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement controls to secure alternate work sites ↗</a>	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Provide privacy training ↗</a>	CMA_0415 - Provide privacy training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Disconnect / Disable Access

ID: FedRAMP Moderate AC-17 (9) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Provide capability to disconnect or disable remote access ↗</a>	CMA_C1066 - Provide capability to disconnect or disable remote access	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Wireless Access

ID: FedRAMP Moderate AC-18 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Document and implement wireless access guidelines ↗</a>	CMA_0190 - Document and implement wireless access guidelines	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Protect wireless access ↗</a>	CMA_0411 - Protect wireless access	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Authentication And Encryption

ID: FedRAMP Moderate AC-18 (1) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Document and implement wireless access guidelines ↗</a>	CMA_0190 - Document and implement wireless access guidelines	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify and authenticate network devices ↗</a>	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Protect wireless access ↗</a>	CMA_0411 - Protect wireless access	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Access Control For Mobile Devices

ID: FedRAMP Moderate AC-19 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define mobile device requirements ↗</a>	CMA_0122 - Define mobile device requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Full Device / Container-Based Encryption

ID: FedRAMP Moderate AC-19 (5) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define mobile device requirements ↗	CMA_0122 - Define mobile device requirements	Manual, Disabled	1.1.0 ↗
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗

## Use Of External Information Systems

ID: FedRAMP Moderate AC-20 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish terms and conditions for accessing resources ↗	CMA_C1076 - Establish terms and conditions for accessing resources	Manual, Disabled	1.1.0 ↗
Establish terms and conditions for processing resources ↗	CMA_C1077 - Establish terms and conditions for processing resources	Manual, Disabled	1.1.0 ↗

## Limits On Authorized Use

ID: FedRAMP Moderate AC-20 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Verify security controls for external information systems ↗	CMA_0541 - Verify security controls for external information systems	Manual, Disabled	1.1.0 ↗

## Portable Storage Devices

ID: FedRAMP Moderate AC-20 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↗
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗

## Information Sharing

ID: FedRAMP Moderate AC-21 Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate information sharing decisions ↗	CMA_0028 - Automate information sharing decisions	Manual, Disabled	1.1.0 ↗
Facilitate information sharing ↗	CMA_0284 - Facilitate information sharing	Manual, Disabled	1.1.0 ↗

## Publicly Accessible Content

ID: FedRAMP Moderate AC-22 Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Designate authorized personnel to post publicly accessible information ↗	CMA_C1083 - Designate authorized personnel to post publicly accessible information	Manual, Disabled	1.1.0 ↗
Review content prior to posting publicly accessible information ↗	CMA_C1085 - Review content prior to posting publicly accessible information	Manual, Disabled	1.1.0 ↗
Review publicly accessible content for nonpublic information ↗	CMA_C1086 - Review publicly accessible content for nonpublic	Manual, Disabled	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal) <a href="#">Train personnel on disclosure of nonpublic information ↗</a>	CMA_C1084 - Train personnel on disclosure of nonpublic information	Manual, Disabled	(GitHub) <a href="#">1.1.0 ↗</a>

## Awareness And Training

### Security Awareness And Training Policy And Procedures

ID: FedRAMP Moderate AT-1 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Document security and privacy training activities ↗</a>	CMA_0198 - Document security and privacy training activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update information security policies ↗</a>	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Awareness Training

ID: FedRAMP Moderate AT-2 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Provide periodic security awareness training ↗</a>	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Provide security training for new users ↗</a>	CMA_0419 - Provide security training for new users	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Provide updated security awareness training ↗</a>	CMA_C1090 - Provide updated security awareness training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Insider Threat

ID: FedRAMP Moderate AT-2 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide security awareness training for insider threats ↗	CMA_0417 - Provide security awareness training for insider threats	Manual, Disabled	1.1.0 ↗

## Role-Based Security Training

ID: FedRAMP Moderate AT-3 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide periodic role-based security training ↗	CMA_C1095 - Provide periodic role-based security training	Manual, Disabled	1.1.0 ↗
Provide role-based security training ↗	CMA_C1094 - Provide role-based security training	Manual, Disabled	1.1.0 ↗
Provide security training before providing access ↗	CMA_0418 - Provide security training before providing access	Manual, Disabled	1.1.0 ↗

## Security Training Records

ID: FedRAMP Moderate AT-4 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗
Monitor security and privacy training completion ↗	CMA_0379 - Monitor security and privacy training completion	Manual, Disabled	1.1.0 ↗
Retain training records ↗	CMA_0456 - Retain training records	Manual, Disabled	1.1.0 ↗

## Audit And Accountability

# Audit And Accountability Policy And Procedures

ID: FedRAMP Moderate AU-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop audit and accountability policies and procedures ↗</a>	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop information security policies and procedures ↗</a>	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Govern policies and procedures ↗</a>	CMA_0292 - Govern policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update information security policies ↗</a>	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Audit Events

ID: FedRAMP Moderate AU-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Determine auditable events ↗</a>	CMA_0137 - Determine auditable events	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Reviews And Updates

ID: FedRAMP Moderate AU-2 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update the events defined in AU-02 ↗</a>	CMA_C1106 - Review and update the events defined in AU-02	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Content Of Audit Records

ID: FedRAMP Moderate AU-3 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↗

## Additional Audit Information

ID: FedRAMP Moderate AU-3 (1) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
Configure Azure Audit capabilities ↗	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	1.1.1 ↗

## Audit Storage Capacity

ID: FedRAMP Moderate AU-4 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
Govern and monitor audit processing activities ↗	CMA_0289 - Govern and monitor audit processing activities	Manual, Disabled	1.1.0 ↗

## Response To Audit Processing Failures

ID: FedRAMP Moderate AU-5 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Govern and monitor audit processing activities ↗	CMA_0289 - Govern and monitor audit processing activities	Manual, Disabled	1.1.0 ↗

## Audit Review, Analysis, And Reporting

ID: FedRAMP Moderate AU-6 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .	AuditIfNotExists, Disabled	6.0.0- preview ↗
[Preview]: Network traffic data collection agent should be installed on Linux virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2- preview ↗
[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2- preview ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for App Service should be enabled ↗	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Azure SQL Database servers should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for DNS should be enabled ↗	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for Key Vault should be enabled ↗	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Resource Manager should be enabled ↗	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for	Azure Defender for servers provides real-time threat protection for server workloads and	AuditIfNotExists, Disabled	1.0.3 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">servers should be enabled ↗</a>	generates hardening recommendations as well as alerts about suspicious activities.		
<a href="#">Azure Defender for SQL servers on machines should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗</a>	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗</a>	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Correlate audit records ↗</a>	CMA_0087 - Correlate audit records	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish requirements for audit review and reporting ↗</a>	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Integrate audit review, analysis, and reporting ↗</a>	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Integrate cloud app security with a siem ↗</a>	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Microsoft Defender for Containers</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should be enabled ↗</a>	protections for your Azure, hybrid, and multi-cloud Kubernetes environments.		
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Network Watcher should be enabled ↗</a>	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Review account provisioning logs ↗</a>	CMA_0460 - Review account provisioning logs	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review administrator assignments weekly ↗</a>	CMA_0461 - Review administrator assignments weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review audit data ↗</a>	CMA_0466 - Review audit data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review cloud identity report overview ↗</a>	CMA_0468 - Review cloud identity report overview	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review controlled folder access events ↗</a>	CMA_0471 - Review controlled folder access events	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review file and folder activity ↗	CMA_0473 - Review file and folder activity	Manual, Disabled	1.1.0 ↗
Review role group changes weekly ↗	CMA_0476 - Review role group changes weekly	Manual, Disabled	1.1.0 ↗

## Process Integration

ID: FedRAMP Moderate AU-6 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Correlate audit records ↗	CMA_0087 - Correlate audit records	Manual, Disabled	1.1.0 ↗
Establish requirements for audit review and reporting ↗	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	1.1.0 ↗
Integrate audit review, analysis, and reporting ↗	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	1.1.0 ↗
Integrate cloud app security with a siem ↗	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	1.1.0 ↗
Review account provisioning logs ↗	CMA_0460 - Review account provisioning logs	Manual, Disabled	1.1.0 ↗
Review administrator assignments weekly ↗	CMA_0461 - Review administrator assignments weekly	Manual, Disabled	1.1.0 ↗
Review audit data ↗	CMA_0466 - Review audit data	Manual, Disabled	1.1.0 ↗
Review cloud identity report overview ↗	CMA_0468 - Review cloud identity report overview	Manual, Disabled	1.1.0 ↗
Review controlled folder access events ↗	CMA_0471 - Review controlled folder access events	Manual, Disabled	1.1.0 ↗
Review file and folder activity ↗	CMA_0473 - Review file and folder	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	activity	Disabled	
Review role group changes weekly ↗	CMA_0476 - Review role group changes weekly	Manual, Disabled	1.1.0 ↗

## Correlate Audit Repositories

ID: FedRAMP Moderate AU-6 (3) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Correlate audit records ↗	CMA_0087 - Correlate audit records	Manual, Disabled	1.1.0 ↗
Integrate cloud app security with a siem ↗	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	1.1.0 ↗

## Audit Reduction And Report Generation

ID: FedRAMP Moderate AU-7 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure audit records are not altered ↗	CMA_C1125 - Ensure audit records are not altered	Manual, Disabled	1.1.0 ↗
Provide audit review, analysis, and reporting capability ↗	CMA_C1124 - Provide audit review, analysis, and reporting capability	Manual, Disabled	1.1.0 ↗

## Automatic Processing

ID: FedRAMP Moderate AU-7 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide capability to process customer-controlled audit records ↴	CMA_C1126 - Provide capability to process customer-controlled audit records	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Time Stamps

ID: FedRAMP Moderate AU-8 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Use system clocks for audit records ↴	CMA_0535 - Use system clocks for audit records	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Synchronization With Authoritative Time Source

ID: FedRAMP Moderate AU-8 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Use system clocks for audit records ↴	CMA_0535 - Use system clocks for audit records	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Protection Of Audit Information

ID: FedRAMP Moderate AU-9 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enable dual or joint authorization ↴	CMA_0226 - Enable dual or joint authorization	Manual, Disabled	<a href="#">1.1.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Protect audit information ↗	CMA_0401 - Protect audit information	Manual, Disabled	1.1.0 ↗

## Audit Backup On Separate Physical Systems / Components

ID: FedRAMP Moderate AU-9 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish backup policies and procedures ↗	CMA_0268 - Establish backup policies and procedures	Manual, Disabled	1.1.0 ↗

## Access By Subset Of Privileged Users

ID: FedRAMP Moderate AU-9 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Protect audit information ↗	CMA_0401 - Protect audit information	Manual, Disabled	1.1.0 ↗

## Audit Record Retention

ID: FedRAMP Moderate AU-11 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adhere to retention periods defined ↗	CMA_0004 - Adhere to retention periods defined	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Retain security policies and procedures ↗	CMA_0454 - Retain security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
SQL servers with auditing to storage account destination should be configured with 90 days retention or higher ↗	<p>For incident investigation purposes, we recommend setting the data retention for your SQL Server' auditing to storage account destination to at least 90 days.</p> <p>Confirm that you are meeting the necessary retention rules for the regions in which you are operating. This is sometimes required for compliance with regulatory standards.</p>	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Audit Generation

ID: FedRAMP Moderate AU-12 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗	<p>Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a>.</p>	AuditIfNotExists, Disabled	<a href="#">6.0.0-preview ↗</a>
[Preview]: Log Analytics extension should be installed on your Linux Azure Arc machines ↗	This policy audits Linux Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	<a href="#">1.0.1-preview ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Log Analytics extension should be installed on your Windows Azure Arc machines ↗	This policy audits Windows Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1-preview ↗
[Preview]: Network traffic data collection agent should be installed on Linux virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
App Service apps should have resource logs enabled ↗	Audit enabling of resource logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised.	AuditIfNotExists, Disabled	2.0.1 ↗
Audit privileged functions ↗	CMA_0019 - Audit privileged functions	Manual, Disabled	1.1.0 ↗
Audit user account status ↗	CMA_0020 - Audit user account status	Manual, Disabled	1.1.0 ↗
Auditing on SQL server should be enabled ↗	Auditing on your SQL Server should be enabled to track database activities across all databases on the server and save them in an audit log.	AuditIfNotExists, Disabled	2.0.0 ↗
Auto provisioning of the Log Analytics agent should be	To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which	AuditIfNotExists, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">enabled on your subscription ↗</a>	reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.		
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Resource Manager should be enabled ↗</a>	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for servers should be enabled ↴	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>
Azure Defender for SQL servers on machines should be enabled ↴	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↴	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↴</a>
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↴	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>
Determine auditable events ↴	CMA_0137 - Determine auditable events	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Guest Configuration extension should be installed on your machines ↴	To ensure secure configurations of in-guest settings of your machine, install the Guest Configuration extension. In-guest settings that the extension monitors include the configuration of the operating system, application configuration or presence, and environment settings. Once installed, in-guest policies will be available such as 'Windows Exploit guard should be enabled'. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Log Analytics agent should be installed on your virtual machine for Azure Security Center monitoring ↴	This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring ↴	Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Microsoft Defender for Containers should be enabled ↴	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Microsoft Defender for Storage should be enabled ↴	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Network Watcher should be enabled ↴	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Resource logs in Azure Data Lake Store should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Azure Stream Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Batch accounts should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Data Lake Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Event Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in IoT Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
Resource logs in Key Vault should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Logic Apps should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.1.0 ↗</a>
Resource logs in Search	Audit enabling of resource logs. This enables you to recreate activity trails to use for	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">services should be enabled ↴</a>	investigation purposes; when a security incident occurs or when your network is compromised		
<a href="#">Resource logs in Service Bus should be enabled ↴</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↴</a>
<a href="#">Review audit data ↴</a>	CMA_0466 - Review audit data	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity ↴</a>	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↴</a>

## Security Assessment And Authorization

### Security Assessment And Authorization Policy And Procedures

ID: FedRAMP Moderate CA-1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review security assessment and authorization policies and procedures ↴</a>	CMA_C1143 - Review security assessment and authorization policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Security Assessments

ID: FedRAMP Moderate CA-2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess Security Controls ↗</a>	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Deliver security assessment results ↗</a>	CMA_C1147 - Deliver security assessment results	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop security assessment plan ↗</a>	CMA_C1144 - Develop security assessment plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Produce Security Assessment report ↗</a>	CMA_C1146 - Produce Security Assessment report	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Independent Assessors

ID: FedRAMP Moderate CA-2 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ independent assessors to conduct security control assessments ↗</a>	CMA_C1148 - Employ independent assessors to conduct security control assessments	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Specialized Assessments

ID: FedRAMP Moderate CA-2 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Select additional testing for security control assessments ↗</a>	CMA_C1149 - Select additional testing for security control assessments	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## External Organizations

ID: FedRAMP Moderate CA-2 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accept assessment results ↗</a>	CMA_C1150 - Accept assessment results	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## System Interconnections

ID: FedRAMP Moderate CA-3 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Require interconnection security agreements ↗</a>	CMA_C1151 - Require interconnection security agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update interconnection security agreements ↗</a>	CMA_0519 - Update interconnection security agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Unclassified Non-National Security System Connections

ID: FedRAMP Moderate CA-3 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement system boundary protection ↗</a>	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Restrictions On External System Connections

ID: FedRAMP Moderate CA-3 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ restrictions on external system interconnections ↗</a>	CMA_C1155 - Employ restrictions on external system interconnections	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Plan Of Action And Milestones

ID: FedRAMP Moderate CA-5 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop POA&amp;M ↗</a>	CMA_C1156 - Develop POA&M	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update POA&amp;M items ↗</a>	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Authorization

ID: FedRAMP Moderate CA-6 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assign an authorizing official (AO) ↗</a>	CMA_C1158 - Assign an authorizing official (AO)	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Ensure resources are authorized ↗</a>	CMA_C1159 - Ensure resources are authorized	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update the security authorization ↗</a>	CMA_C1160 - Update the security authorization	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Continuous Monitoring

ID: FedRAMP Moderate CA-7 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure detection whitelist ↗	CMA_0068 - Configure detection whitelist	Manual, Disabled	1.1.0 ↗
Turn on sensors for endpoint security solution ↗	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	1.1.0 ↗
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	1.1.0 ↗

## Independent Assessment

ID: FedRAMP Moderate CA-7 (1) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ independent assessors for continuous monitoring ↗	CMA_C1168 - Employ independent assessors for continuous monitoring	Manual, Disabled	1.1.0 ↗

## Independent Penetration Agent Or Team

ID: FedRAMP Moderate CA-8 (1) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ independent team for penetration testing ↗	CMA_C1171 - Employ independent team for penetration testing	Manual, Disabled	1.1.0 ↗

## Internal System Connections

ID: FedRAMP Moderate CA-9 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Check for privacy and security compliance before establishing internal connections ↗</a>	CMA_0053 - Check for privacy and security compliance before establishing internal connections	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Configuration Management

## Configuration Management Policy And Procedures

ID: FedRAMP Moderate CM-1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update configuration management policies and procedures ↗</a>	CMA_C1175 - Review and update configuration management policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Baseline Configuration

ID: FedRAMP Moderate CM-2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Configure actions for noncompliant devices ↗</a>	CMA_0062 - Configure actions for noncompliant devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop and maintain baseline configurations ↗</a>	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce security configuration settings ↗</a>	CMA_0249 - Enforce security configuration settings	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a configuration control board ↗</a>	CMA_0254 - Establish a configuration control board	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and document a configuration management plan ↗</a>	CMA_0264 - Establish and document a configuration	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	management plan		
Implement an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	1.1.0 ↗

## Automation Support For Accuracy / Currency

ID: FedRAMP Moderate CM-2 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure actions for noncompliant devices ↗	CMA_0062 - Configure actions for noncompliant devices	Manual, Disabled	1.1.0 ↗
Develop and maintain baseline configurations ↗	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	1.1.0 ↗
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗
Establish a configuration control board ↗	CMA_0254 - Establish a configuration control board	Manual, Disabled	1.1.0 ↗
Establish and document a configuration management plan ↗	CMA_0264 - Establish and document a configuration management plan	Manual, Disabled	1.1.0 ↗
Implement an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	1.1.0 ↗

## Retention Of Previous Configurations

ID: FedRAMP Moderate CM-2 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Retain previous versions of baseline configs ↗	CMA_C1181 - Retain previous versions of baseline configs	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Configure Systems, Components, Or Devices For High-Risk Areas

ID: FedRAMP Moderate CM-2 (7) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure security safeguards not needed when the individuals return ↗	CMA_C1183 - Ensure security safeguards not needed when the individuals return	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Not allow for information systems to accompany with individuals ↗	CMA_C1182 - Not allow for information systems to accompany with individuals	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Configuration Change Control

ID: FedRAMP Moderate CM-3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and maintain a vulnerability management standard ↗	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Impact Analysis

ID: FedRAMP Moderate CM-4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and maintain a vulnerability management standard ↗	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform audit for configuration	CMA_0390 - Perform audit for	Manual,	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">change control ↗</a>	configuration change control	Disabled	

## Access Restrictions For Change

ID: FedRAMP Moderate CM-5 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Establish and document change control processes ↗</a>	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Access Enforcement / Auditing

ID: FedRAMP Moderate CM-5 (1) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Enforce and audit access restrictions ↗</a>	CMA_C1203 - Enforce and audit access restrictions	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Signed Components

ID: FedRAMP Moderate CM-5 (3) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Restrict unauthorized software and firmware installation ↗</a>	CMA_C1205 - Restrict unauthorized software and firmware installation	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Limit Production / Operational Privileges

ID: FedRAMP Moderate CM-5 (5) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Limit privileges to make changes in production environment ↗</a>	CMA_C1206 - Limit privileges to make changes in production environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and reevaluate privileges ↗</a>	CMA_C1207 - Review and reevaluate privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Configuration Settings

ID: FedRAMP Moderate CM-6 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Deprecated]: Function apps should have 'Client Certificates (Incoming client certificates)' enabled ↗</a>	Client certificates allow for the app to request a certificate for incoming requests. Only clients with valid certificates will be able to reach the app. This policy has been replaced by a new policy with the same name because Http 2.0 doesn't support client certificates.	Audit, Disabled	<a href="#">3.1.0-deprecated ↗</a>
<a href="#">App Service apps should have Client Certificates (Incoming client certificates) enabled ↗</a>	Client certificates allow for the app to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the app. This policy applies to apps with Http version set to 1.1.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">App Service apps should have remote debugging turned off ↗</a>	Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">App Service apps should not</a>	Cross-Origin Resource Sharing (CORS) should not allow all domains to access	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
have CORS configured to allow every resource to access your apps ↗	your app. Allow only required domains to interact with your app.		
Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your clusters ↗	Azure Policy Add-on for Kubernetes service (AKS) extends Gatekeeper v3, an admission controller webhook for Open Policy Agent (OPA), to apply at-scale enforcements and safeguards on your clusters in a centralized, consistent manner.	Audit, Disabled	1.0.2 ↗
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗
Function apps should have remote debugging turned off ↗	Remote debugging requires inbound ports to be opened on Function apps. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0 ↗
Function apps should not have CORS configured to allow every resource to access your apps ↗	Cross-Origin Resource Sharing (CORS) should not allow all domains to access your Function app. Allow only required domains to interact with your Function app.	AuditIfNotExists, Disabled	2.0.0 ↗
Kubernetes cluster containers CPU and memory resource limits should not exceed the specified limits ↗	Enforce container CPU and memory resource limits to prevent resource exhaustion attacks in a Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	9.1.0 ↗
Kubernetes cluster containers should not	Block pod containers from sharing the host process ID namespace and host IPC namespace in a Kubernetes cluster. This recommendation is part of CIS 5.2.2 and	audit, Audit, deny, Deny, disabled, Disabled	5.1.0 ↗

Name	Description	Effect(s)	Version
			(GitHub)
share host process ID or (Azure portal) host IPC namespace ↴	CIS 5.2.3 which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .		
Kubernetes cluster containers should only use allowed AppArmor profiles ↴	Containers should only use allowed AppArmor profiles in a Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.1 ↴
Kubernetes cluster containers should only use allowed capabilities ↴	Restrict the capabilities to reduce the attack surface of containers in a Kubernetes cluster. This recommendation is part of CIS 5.2.8 and CIS 5.2.9 which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.0 ↴
Kubernetes cluster containers should only use allowed images ↴	Use images from trusted registries to reduce the Kubernetes cluster's exposure risk to unknown vulnerabilities, security issues and malicious images. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	9.1.1 ↴
Kubernetes cluster containers should run with a read only root file system ↴	Run containers with a read only root file system to protect from changes at runtime with malicious binaries being added to PATH in a Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.0 ↴
Kubernetes cluster pod hostPath volumes should only use allowed host paths ↴	Limit pod HostPath volume mounts to the allowed host paths in a Kubernetes Cluster. This policy is generally available for Kubernetes Service (AKS), and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.1 ↴

Name  (Azure portal)	Description	Effect(s)	Version  (GitHub)
<a href="#">Kubernetes cluster pods and containers should only run with approved user and group IDs ↗</a>	Control the user, primary group, supplemental group and file system group IDs that pods and containers can use to run in a Kubernetes Cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.1 ↗
<a href="#">Kubernetes cluster pods should only use approved host network and port range ↗</a>	Restrict pod access to the host network and the allowable host port range in a Kubernetes cluster. This recommendation is part of CIS 5.2.4 which is intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.0 ↗
<a href="#">Kubernetes cluster services should listen only on allowed ports ↗</a>	Restrict services to listen only on allowed ports to secure access to the Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	8.1.0 ↗
<a href="#">Kubernetes cluster should not allow privileged containers ↗</a>	Do not allow privileged containers creation in a Kubernetes cluster. This recommendation is part of CIS 5.2.1 which is intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	9.1.0 ↗
<a href="#">Kubernetes clusters should not allow container privilege escalation ↗</a>	Do not allow containers to run with privilege escalation to root in a Kubernetes cluster. This recommendation is part of CIS 5.2.5 which is intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more	audit, Audit, deny, Deny, disabled, Disabled	7.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .		
Linux machines should meet requirements for the Azure compute security baseline ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if the machine is not configured correctly for one of the recommendations in the Azure compute security baseline.	AuditIfNotExists, Disabled	2.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗
Windows machines should meet requirements of the Azure compute security baseline ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if the machine is not configured correctly for one of the recommendations in the Azure compute security baseline.	AuditIfNotExists, Disabled	2.0.0 ↗

## Automated Central Management / Application / Verification

ID: FedRAMP Moderate CM-6 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗
Govern compliance of cloud service providers ↗	CMA_0290 - Govern compliance of cloud service providers	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

## Least Functionality

## ID: FedRAMP Moderate CM-7 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications should be enabled on your machines ↗</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Azure Defender for servers should be enabled ↗</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

## Prevent Program Execution

### ID: FedRAMP Moderate CM-7 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should be enabled on your machines ↗</a>	rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.		
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Authorized Software / Whitelisting

ID: FedRAMP Moderate CM-7 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications should be enabled on your machines ↗</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

# Information System Component Inventory

ID: FedRAMP Moderate CM-8 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Create a data inventory ↗</a>	CMA_0096 - Create a data inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Maintain records of processing of personal data ↗</a>	CMA_0353 - Maintain records of processing of personal data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Updates During Installations / Removals

ID: FedRAMP Moderate CM-8 (1) Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Create a data inventory ↗</a>	CMA_0096 - Create a data inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Maintain records of processing of personal data ↗</a>	CMA_0353 - Maintain records of processing of personal data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Unauthorized Component Detection

ID: FedRAMP Moderate CM-8 (3) Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Enable detection of network devices ↗</a>	CMA_0220 - Enable detection of network devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Set automated notifications for new and trending cloud applications in your organization ↗</a>	CMA_0495 - Set automated notifications for new and trending cloud applications in your organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Configuration Management Plan

ID: FedRAMP Moderate CM-9 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Create configuration plan protection ↗	CMA_C1233 - Create configuration plan protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and maintain baseline configurations ↗	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop configuration item identification plan ↗	CMA_C1231 - Develop configuration item identification plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop configuration management plan ↗	CMA_C1232 - Develop configuration management plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish and document a configuration management plan ↗	CMA_0264 - Establish and document a configuration management plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Software Usage Restrictions

ID: FedRAMP Moderate CM-10 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adaptive application controls for defining safe applications should be enabled on your machines ↗	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Allowlist rules in your adaptive application control policy should be updated ↗	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Require compliance with intellectual property rights ↗	CMA_0432 - Require compliance with intellectual property rights	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Track software license usage ↗	CMA_C1235 - Track software license usage	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Open Source Software

ID: FedRAMP Moderate CM-10 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Restrict use of open source software ↗	CMA_C1237 - Restrict use of open source software	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## User-Installed Software

ID: FedRAMP Moderate CM-11 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adaptive application controls for defining safe	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">applications should be enabled on your machines ↗</a>	machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.		
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Contingency Planning

### Contingency Planning Policy And Procedures

ID: FedRAMP Moderate CP-1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update contingency planning policies and procedures ↗</a>	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Contingency Plan

ID: FedRAMP Moderate CP-2 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Communicate contingency plan changes ↗	CMA_C1249 - Communicate contingency plan changes	Manual, Disabled	1.1.0 ↗
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	1.1.0 ↗
Develop and document a business continuity and disaster recovery plan ↗	CMA_0146 - Develop and document a business continuity and disaster recovery plan	Manual, Disabled	1.1.0 ↗
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0 ↗
Develop contingency planning policies and procedures ↗	CMA_0156 - Develop contingency planning policies and procedures	Manual, Disabled	1.1.0 ↗
Distribute policies and procedures ↗	CMA_0185 - Distribute policies and procedures	Manual, Disabled	1.1.0 ↗
Review contingency plan ↗	CMA_C1247 - Review contingency plan	Manual, Disabled	1.1.0 ↗
Update contingency plan ↗	CMA_C1248 - Update contingency plan	Manual, Disabled	1.1.0 ↗

## Coordinate With Related Plans

ID: FedRAMP Moderate CP-2 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	1.1.0 ↗

## Capacity Planning

ID: FedRAMP Moderate CP-2 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct capacity planning ↗	CMA_C1252 - Conduct capacity planning	Manual, Disabled	1.1.0 ↗

## Resume Essential Missions / Business Functions

ID: FedRAMP Moderate CP-2 (3) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Plan for resumption of essential business functions ↗	CMA_C1253 - Plan for resumption of essential business functions	Manual, Disabled	1.1.0 ↗

## Identify Critical Assets

ID: FedRAMP Moderate CP-2 (8) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform a business impact assessment and application criticality assessment ↗	CMA_0386 - Perform a business impact assessment and application criticality assessment	Manual, Disabled	1.1.0 ↗

## Contingency Training

ID: FedRAMP Moderate CP-3 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide contingency training ↗	CMA_0412 - Provide contingency training	Manual, Disabled	1.1.0 ↗

# Contingency Plan Testing

ID: FedRAMP Moderate CP-4 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Initiate contingency plan testing corrective actions ↗</a>	CMA_C1263 - Initiate contingency plan testing corrective actions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review the results of contingency plan testing ↗</a>	CMA_C1262 - Review the results of contingency plan testing	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Test the business continuity and disaster recovery plan ↗</a>	CMA_0509 - Test the business continuity and disaster recovery plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Coordinate With Related Plans

ID: FedRAMP Moderate CP-4 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Coordinate contingency plans with related plans ↗</a>	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Alternate Storage Site

ID: FedRAMP Moderate CP-6 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Ensure alternate storage site safeguards are equivalent to primary site ↗</a>	CMA_C1268 - Ensure alternate storage site safeguards are equivalent to primary site	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish alternate storage site to store and retrieve backup information ↗	CMA_C1267 - Establish alternate storage site to store and retrieve backup information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Geo-redundant backup should be enabled for Azure Database for MariaDB ↗	Azure Database for MariaDB allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
Geo-redundant backup should be enabled for Azure Database for MySQL ↗	Azure Database for MySQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
Geo-redundant backup should be enabled for Azure Database for PostgreSQL ↗	Azure Database for PostgreSQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
Geo-redundant storage should be enabled for Storage Accounts ↗	Use geo-redundancy to create highly available applications	Audit, Disabled	<a href="#">1.0.0 ↗</a>
Long-term geo-redundant backup should be enabled	This policy audits any Azure SQL Database with long-term geo-redundant backup not enabled.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
for Azure SQL Databases ↗			

## Separation From Primary Site

ID: FedRAMP Moderate CP-6 (1) Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Create separate alternate and primary storage sites ↗	CMA_C1269 - Create separate alternate and primary storage sites	Manual, Disabled	1.1.0 ↗
Geo-redundant backup should be enabled for Azure Database for MariaDB ↗	Azure Database for MariaDB allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	1.0.1 ↗
Geo-redundant backup should be enabled for Azure Database for MySQL ↗	Azure Database for MySQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	1.0.1 ↗
Geo-redundant backup should be enabled for Azure Database for PostgreSQL ↗	Azure Database for PostgreSQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in	Audit, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.		
Geo-redundant storage should be enabled for Storage Accounts <a href="#">↗</a>	Use geo-redundancy to create highly available applications	Audit, Disabled	<a href="#">1.0.0 ↗</a>
Long-term geo-redundant backup should be enabled for Azure SQL Databases <a href="#">↗</a>	This policy audits any Azure SQL Database with long-term geo-redundant backup not enabled.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

## Accessibility

ID: FedRAMP Moderate CP-6 (3) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Identify and mitigate potential issues at alternate storage site <a href="#">↗</a>	CMA_C1271 - Identify and mitigate potential issues at alternate storage site	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Alternate Processing Site

ID: FedRAMP Moderate CP-7 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit virtual machines without disaster recovery configured <a href="#">↗</a>	Audit virtual machines which do not have disaster recovery configured. To learn more about disaster recovery, visit <a href="https://aka.ms/asr-doc">https://aka.ms/asr-doc</a> <a href="#">↗</a> .	auditIfNotExists	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗

## Separation From Primary Site

ID: FedRAMP Moderate CP-7 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗

## Accessibility

ID: FedRAMP Moderate CP-7 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗

## Priority Of Service

ID: FedRAMP Moderate CP-7 (3) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗
Establish requirements for internet service providers ↗	CMA_0278 - Establish requirements for internet service providers	Manual, Disabled	1.1.0 ↗

# Priority Of Service Provisions

ID: FedRAMP Moderate CP-8 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish requirements for internet service providers ↗</a>	CMA_0278 - Establish requirements for internet service providers	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Information System Backup

ID: FedRAMP Moderate CP-9 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Azure Backup should be enabled for Virtual Machines ↗</a>	Ensure protection of your Azure Virtual Machines by enabling Azure Backup. Azure Backup is a secure and cost effective data protection solution for Azure.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Conduct backup of information system documentation ↗</a>	CMA_C1289 - Conduct backup of information system documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish backup policies and procedures ↗</a>	CMA_0268 - Establish backup policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Geo-redundant backup should be enabled for Azure Database for MariaDB ↗</a>	Azure Database for MariaDB allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Geo-redundant backup should be</a>	Azure Database for MySQL allows you to choose the redundancy option for your database server. It can be set to a geo-	Audit, Disabled	<a href="#">1.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">enabled for Azure Database for MySQL ↴</a>	redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.		
<a href="#">Geo-redundant backup should be enabled for Azure Database for PostgreSQL ↴</a>	Azure Database for PostgreSQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↴</a>
<a href="#">Implement controls to secure all media ↴</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Key vaults should have deletion protection enabled ↴</a>	Malicious deletion of a key vault can lead to permanent data loss. You can prevent permanent data loss by enabling purge protection and soft delete. Purge protection protects you from insider attacks by enforcing a mandatory retention period for soft deleted key vaults. No one inside your organization or Microsoft will be able to purge your key vaults during the soft delete retention period. Keep in mind that key vaults created after September 1st 2019 have soft-delete enabled by default.	Audit, Deny, Disabled	<a href="#">2.1.0 ↴</a>
<a href="#">Key vaults should have soft delete enabled ↴</a>	Deleting a key vault without soft delete enabled permanently deletes all secrets, keys, and certificates stored in the key vault. Accidental deletion of a key vault can lead to permanent data loss. Soft delete allows you to recover an accidentally deleted key vault for a configurable retention period.	Audit, Deny, Disabled	<a href="#">3.0.0 ↴</a>

## Separate Storage For Critical Information

ID: FedRAMP Moderate CP-9 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Separately store backup information ↗</a>	CMA_C1293 - Separately store backup information	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information System Recovery And Reconstitution

ID: FedRAMP Moderate CP-10 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Recover and reconstitute resources after any disruption ↗</a>	CMA_C1295 - Recover and reconstitute resources after any disruption	Manual, Disabled	<a href="#">1.1.1 ↗</a>

## Transaction Recovery

ID: FedRAMP Moderate CP-10 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement transaction based recovery ↗</a>	CMA_C1296 - Implement transaction based recovery	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Identification And Authentication

### Identification And Authentication Policy And Procedures

ID: FedRAMP Moderate IA-1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update identification and authentication policies and procedures ↴	CMA_C1299 - Review and update identification and authentication policies and procedures	Manual, Disabled	1.1.0 ↴

## Identification And Authentication (Organizational Users)

ID: FedRAMP Moderate IA-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Accounts with owner permissions on Azure resources should be MFA enabled ↴	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	1.0.0 ↴
Accounts with read permissions on Azure resources should be MFA enabled ↴	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	1.0.0 ↴
Accounts with write permissions on Azure resources should be MFA enabled ↴	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	1.0.0 ↴
An Azure Active Directory administrator should be provisioned for SQL servers ↴	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	1.0.0 ↴
App Service apps should use managed identity ↴	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	3.0.0 ↴
Cognitive Services accounts should have local authentication methods disabled ↴	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for	Audit, Deny, Disabled	1.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> .		
Enforce user uniqueness <a href="#">🔗</a>	CMA_0250 - Enforce user uniqueness	Manual, Disabled	<a href="#">1.1.0</a> <a href="#">🔗</a>
Function apps should use managed identity <a href="#">🔗</a>	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0</a> <a href="#">🔗</a>
Service Fabric clusters should only use Azure Active Directory for client authentication <a href="#">🔗</a>	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	<a href="#">1.1.0</a> <a href="#">🔗</a>
Support personal verification credentials issued by legal authorities <a href="#">🔗</a>	CMA_0507 - Support personal verification credentials issued by legal authorities	Manual, Disabled	<a href="#">1.1.0</a> <a href="#">🔗</a>

## Network Access To Privileged Accounts

ID: FedRAMP Moderate IA-2 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Accounts with owner permissions on Azure resources should be MFA enabled <a href="#">🔗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0</a> <a href="#">🔗</a>
Accounts with write permissions on Azure resources should be MFA enabled <a href="#">🔗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0</a> <a href="#">🔗</a>
Adopt biometric authentication mechanisms <a href="#">🔗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0</a> <a href="#">🔗</a>

# Network Access To Non-Privileged Accounts

ID: FedRAMP Moderate IA-2 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accounts with read permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Local Access To Privileged Accounts

ID: FedRAMP Moderate IA-2 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Group Authentication

ID: FedRAMP Moderate IA-2 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Require use of individual authenticators ↗</a>	CMA_C1305 - Require use of individual authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Remote Access - Separate Device

ID: FedRAMP Moderate IA-2 (11) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify and authenticate network devices ↗</a>	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Acceptance Of Piv Credentials

ID: FedRAMP Moderate IA-2 (12) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Support personal verification credentials issued by legal authorities ↗</a>	CMA_0507 - Support personal verification credentials issued by legal authorities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Identifier Management

ID: FedRAMP Moderate IA-4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">An Azure Active Directory administrator should be provisioned for SQL servers ↗</a>	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">App Service apps should use managed identity ↗</a>	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign system identifiers ↴	CMA_0018 - Assign system identifiers	Manual, Disabled	1.1.0 ↴
Cognitive Services accounts should have local authentication methods disabled ↴	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> .	Audit, Deny, Disabled	1.0.0 ↴
Function apps should use managed identity ↴	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	3.0.0 ↴
Prevent identifier reuse for the defined time period ↴	CMA_C1314 - Prevent identifier reuse for the defined time period	Manual, Disabled	1.1.0 ↴
Service Fabric clusters should only use Azure Active Directory for client authentication ↴	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	1.1.0 ↴

## Identify User Status

ID: FedRAMP Moderate IA-4 (4) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Identify status of individual users ↴	CMA_C1316 - Identify status of individual users	Manual, Disabled	1.1.0 ↴

## Authenticator Management

ID: FedRAMP Moderate IA-5 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Certificates should have the specified maximum validity period ↴	Manage your organizational compliance requirements by specifying the maximum amount of time that a certificate can be valid within your key vault.	audit, Audit, deny, Deny, disabled, Disabled	2.2.0-preview ↴
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↴	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴.	modify	4.0.0 ↴
Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↴	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴.	modify	4.0.0 ↴
Audit Linux machines that do not have the passwd file permissions set to 0644 ↴	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴. Machines are non-compliant if Linux machines that do not have the passwd file permissions set to 0644	AuditIfNotExists, Disabled	3.0.0 ↴
Audit Windows machines that do not store passwords using reversible encryption ↴	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴. Machines are non-compliant if Windows machines that do not store passwords using reversible encryption	AuditIfNotExists, Disabled	2.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authentication to Linux machines should require SSH keys ↗	Although SSH itself provides an encrypted connection, using passwords with SSH still leaves the VM vulnerable to brute-force attacks. The most secure option for authenticating to an Azure Linux virtual machine over SSH is with a public-private key pair, also known as SSH keys. Learn more: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed">https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed</a> .	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↗	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	deployIfNotExists	<a href="#">3.0.0 ↗</a>
Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs ↗	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	deployIfNotExists	<a href="#">1.2.0 ↗</a>
Establish authenticator types and processes ↗	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish procedures for initial authenticator distribution ↗	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement training for protecting authenticators ↗	CMA_0329 - Implement training for protecting authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Key Vault keys should have an expiration date ↗	Cryptographic keys should have a defined expiration date and not be permanent. Keys that are valid forever provide a potential attacker with more time to compromise the key. It is a recommended security practice to set expiration dates on cryptographic keys.	Audit, Deny, Disabled	<a href="#">1.0.2 ↗</a>
Key Vault secrets should have an expiration date ↗	Secrets should have a defined expiration date and not be permanent. Secrets that are valid forever provide a potential attacker with more time to compromise them. It is a recommended security practice to set expiration dates on secrets.	Audit, Deny, Disabled	<a href="#">1.0.2 ↗</a>
Manage authenticator lifetime and reuse ↗	CMA_0355 - Manage authenticator lifetime and reuse	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage Authenticators ↗	CMA_C1321 - Manage Authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Refresh authenticators ↗	CMA_0425 - Refresh authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Reissue authenticators for changed groups and accounts ↗	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Password-Based Authentication

ID: FedRAMP Moderate IA-5 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	4.0.0 ↗
Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	4.0.0 ↗
Audit Linux machines that do not have the passwd file permissions set to 0644 ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Linux machines that do not have the passwd file permissions set to 0644	AuditIfNotExists, Disabled	3.0.0 ↗
Audit Windows machines that allow re-use of the passwords after the specified number of unique passwords ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that allow re-use of the passwords after the specified number of unique passwords. Default value for unique passwords is 24	AuditIfNotExists, Disabled	2.1.0 ↗
Audit Windows machines that do not have the maximum password age set to specified number of days ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not have the maximum password age set to specified number of days. Default value for maximum password age is 70 days	AuditIfNotExists, Disabled	2.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit Windows machines that do not have the minimum password age set to specified number of days ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Windows machines that do not have the minimum password age set to specified number of days. Default value for minimum password age is 1 day	AuditIfNotExists, Disabled	<a href="#">2.1.0 ↗</a>
<a href="#">Audit Windows machines that do not have the password complexity setting enabled ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Windows machines that do not have the password complexity setting enabled	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Audit Windows machines that do not restrict the minimum password length to specified number of characters ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Windows machines that do not restrict the minimum password length to specified number of characters. Default value for minimum password length is 14 characters	AuditIfNotExists, Disabled	<a href="#">2.1.0 ↗</a>
<a href="#">Audit Windows machines that do not store passwords using reversible encryption ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Windows machines that do not store passwords using reversible encryption	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↗</a>	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	deployIfNotExists	<a href="#">3.0.0 ↗</a>
<a href="#">Deploy the Windows Guest Configuration extension to enable Guest</a>	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for	deployIfNotExists	<a href="#">1.2.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configuration assignments on Windows VMs ↗	all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.		
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0</a> ↗
Establish a password policy ↗	CMA_0256 - Establish a password policy	Manual, Disabled	<a href="#">1.1.0</a> ↗
Implement parameters for memorized secret verifiers ↗	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	<a href="#">1.1.0</a> ↗
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	<a href="#">1.1.0</a> ↗

## Pki-Based Authentication

ID: FedRAMP Moderate IA-5 (2) Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Bind authenticators and identities dynamically ↗	CMA_0035 - Bind authenticators and identities dynamically	Manual, Disabled	<a href="#">1.1.0</a> ↗
Establish authenticator types and processes ↗	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	<a href="#">1.1.0</a> ↗
Establish parameters for searching secret authenticators and verifiers ↗	CMA_0274 - Establish parameters for searching secret authenticators and verifiers	Manual, Disabled	<a href="#">1.1.0</a> ↗
Establish procedures for initial authenticator distribution ↗	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	<a href="#">1.1.0</a> ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Map authenticated identities to individuals ↗	CMA_0372 - Map authenticated identities to individuals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Restrict access to private keys ↗	CMA_0445 - Restrict access to private keys	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## In-Person Or Trusted Third-Party Registration

ID: FedRAMP Moderate IA-5 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Distribute authenticators ↗	CMA_0184 - Distribute authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Support For Password Strength Determination

ID: FedRAMP Moderate IA-5 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a password policy ↗	CMA_0256 - Establish a password policy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement parameters for memorized secret verifiers ↗	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Protection Of Authenticators

ID: FedRAMP Moderate IA-5 (6) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure authorized users protect provided authenticators ↗	CMA_C1339 - Ensure authorized users protect provided authenticators	Manual, Disabled	1.1.0 ↗

## No Embedded Unencrypted Static Authenticators

ID: FedRAMP Moderate IA-5 (7) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure there are no unencrypted static authenticators ↗	CMA_C1340 - Ensure there are no unencrypted static authenticators	Manual, Disabled	1.1.0 ↗

## Hardware Token-Based Authentication

ID: FedRAMP Moderate IA-5 (11) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Satisfy token quality requirements ↗	CMA_0487 - Satisfy token quality requirements	Manual, Disabled	1.1.0 ↗

## Authenticator Feedback

ID: FedRAMP Moderate IA-6 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Obscure feedback information during authentication process ↗	CMA_C1344 - Obscure feedback information during authentication process	Manual, Disabled	1.1.0 ↗

## Cryptographic Module Authentication

ID: FedRAMP Moderate IA-7 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authenticate to cryptographic module ↗	CMA_0021 - Authenticate to cryptographic module	Manual, Disabled	1.1.0 ↗

## Identification And Authentication (Non- Organizational Users)

ID: FedRAMP Moderate IA-8 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Identify and authenticate non- organizational users ↗	CMA_C1346 - Identify and authenticate non-organizational users	Manual, Disabled	1.1.0 ↗

## Acceptance Of Piv Credentials From Other Agencies

ID: FedRAMP Moderate IA-8 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Accept PIV credentials ↗	CMA_C1347 - Accept PIV credentials	Manual, Disabled	1.1.0 ↗

# Acceptance Of Third-Party Credentials

ID: FedRAMP Moderate IA-8 (2) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Accept only FICAM-approved third-party credentials ↗</a>	CMA_C1348 - Accept only FICAM-approved third-party credentials	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Use Of Ficam-Approved Products

ID: FedRAMP Moderate IA-8 (3) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Employ FICAM-approved resources to accept third-party credentials ↗</a>	CMA_C1349 - Employ FICAM-approved resources to accept third-party credentials	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Use Of Ficam-Issued Profiles

ID: FedRAMP Moderate IA-8 (4) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Conform to FICAM-issued profiles ↗</a>	CMA_C1350 - Conform to FICAM-issued profiles	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Incident Response

## Incident Response Policy And Procedures

ID: FedRAMP Moderate IR-1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update incident response policies and procedures ↗</a>	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Incident Response Training

ID: FedRAMP Moderate IR-2 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Provide information spillage training ↗</a>	CMA_0413 - Provide information spillage training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Incident Response Testing

ID: FedRAMP Moderate IR-3 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Conduct incident response testing ↗</a>	CMA_0060 - Conduct incident response testing	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish an information security program ↗</a>	CMA_0263 - Establish an information security program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Run simulation attacks ↗</a>	CMA_0486 - Run simulation attacks	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Coordination With Related Plans

ID: FedRAMP Moderate IR-3 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct incident response testing ↗	CMA_0060 - Conduct incident response testing	Manual, Disabled	1.1.0 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	1.1.0 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗

## Incident Handling

ID: FedRAMP Moderate IR-4 Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess information security events ↗	CMA_0013 - Assess information security events	Manual, Disabled	1.1.0 ↗
Azure Defender for App Service should be enabled ↗	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Azure SQL Database servers should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for DNS should be enabled ↗	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for Key Vault should be enabled ↗	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Resource Manager should be enabled ↗	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for SQL servers on machines should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	2.0.1 ↗
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↗
Coordinate contingency	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
plans with related plans ↗			
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Develop security safeguards ↗	CMA_0161 - Develop security safeguards	Manual, Disabled	1.1.0 ↗
Email notification for high severity alerts should be enabled ↗	To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, enable email notifications for high severity alerts in Security Center.	AuditIfNotExists, Disabled	1.0.1 ↗
Email notification to subscription owner for high severity alerts should be enabled ↗	To ensure your subscription owners are notified when there is a potential security breach in their subscription, set email notifications to subscription owners for high severity alerts in Security Center.	AuditIfNotExists, Disabled	2.0.0 ↗
Enable network protection ↗	CMA_0238 - Enable network protection	Manual, Disabled	1.1.0 ↗
Eradicate contaminated information ↗	CMA_0253 - Eradicate contaminated information	Manual, Disabled	1.1.0 ↗
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	1.1.0 ↗
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗
Maintain incident response plan ↗	CMA_0352 - Maintain incident response plan	Manual, Disabled	1.1.0 ↗
Microsoft Defender for Containers should be enabled ↗	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	1.0.0 ↗
Microsoft Defender for Storage	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Storage should be enabled ↗	data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.		
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Subscriptions should have a contact email address for security issues ↗	To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, set a security contact to receive email notifications from Security Center.	AuditIfNotExists, Disabled	1.0.1 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

## Automated Incident Handling Processes

ID: FedRAMP Moderate IR-4 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Enable network protection ↗	CMA_0238 - Enable network protection	Manual, Disabled	1.1.0 ↗
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗

## Incident Monitoring

ID: FedRAMP Moderate IR-5 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Resource Manager should be enabled ↗</a>	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for servers</a>	Azure Defender for servers provides real-time threat protection for server workloads and	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should be enabled ↗</a>	generates hardening recommendations as well as alerts about suspicious activities.		
<a href="#">Azure Defender for SQL servers on machines should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗</a>	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗</a>	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Email notification for high severity alerts should be enabled ↗</a>	To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, enable email notifications for high severity alerts in Security Center.	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Email notification to subscription owner for high severity alerts should be enabled ↗</a>	To ensure your subscription owners are notified when there is a potential security breach in their subscription, set email notifications to subscription owners for high severity alerts in Security Center.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Microsoft Defender for Containers should be enabled ↗</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.			
Subscriptions should have a contact email address for security issues ↗	To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, set a security contact to receive email notifications from Security Center.	AuditIfNotExists, Disabled	1.0.1 ↗

## Automated Reporting

ID: FedRAMP Moderate IR-6 (1) Ownership: Shared

[ ] Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Document security operations ↗	CMA_0202 - Document security operations	Manual, Disabled	1.1.0 ↗

## Incident Response Assistance

ID: FedRAMP Moderate IR-7 Ownership: Shared

[ ] Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Document security operations ↗	CMA_0202 - Document security operations	Manual, Disabled	1.1.0 ↗

## Automation Support For Availability Of Information / Support

ID: FedRAMP Moderate IR-7 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enable network protection ↗	CMA_0238 - Enable network protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Eradicate contaminated information ↗	CMA_0253 - Eradicate contaminated information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	<a href="#">1.1.0 ↗</a>
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Coordination With External Providers

ID: FedRAMP Moderate IR-7 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish relationship between incident response capability and external providers ↗	CMA_C1376 - Establish relationship between incident response capability and external providers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Identify incident response personnel ↗	CMA_0301 - Identify incident response personnel	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Incident Response Plan

ID: FedRAMP Moderate IR-8 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess information security events ↗	CMA_0013 - Assess information security events	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗
Maintain data breach records ↗	CMA_0351 - Maintain data breach records	Manual, Disabled	1.1.0 ↗
Maintain incident response plan ↗	CMA_0352 - Maintain incident response plan	Manual, Disabled	1.1.0 ↗
Protect incident response plan ↗	CMA_0405 - Protect incident response plan	Manual, Disabled	1.1.0 ↗

## Information Spillage Response

ID: FedRAMP Moderate IR-9 Ownership: Shared

↔ Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Alert personnel of information spillage ↗	CMA_0007 - Alert personnel of information spillage	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Eradicate contaminated information ↗	CMA_0253 - Eradicate contaminated information	Manual, Disabled	1.1.0 ↗
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	1.1.0 ↗
Identify contaminated systems and components ↗	CMA_0300 - Identify contaminated systems and components	Manual, Disabled	1.1.0 ↗
Identify spilled information ↗	CMA_0303 - Identify spilled information	Manual, Disabled	1.1.0 ↗
Isolate information spills ↗	CMA_0346 - Isolate information	Manual,	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
	spills	Disabled	

## Responsible Personnel

ID: FedRAMP Moderate IR-9 (1) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Identify incident response personnel ↗</a>	CMA_0301 - Identify incident response personnel	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Training

ID: FedRAMP Moderate IR-9 (2) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Provide information spillage training ↗</a>	CMA_0413 - Provide information spillage training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Post-Spill Operations

ID: FedRAMP Moderate IR-9 (3) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Develop spillage response procedures ↗</a>	CMA_0162 - Develop spillage response procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Exposure To Unauthorized Personnel

ID: FedRAMP Moderate IR-9 (4) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop security safeguards ↗</a>	CMA_0161 - Develop security safeguards	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Maintenance

### System Maintenance Policy And Procedures

ID: FedRAMP Moderate MA-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update system maintenance policies and procedures ↗</a>	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

### Controlled Maintenance

ID: FedRAMP Moderate MA-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ a media sanitization mechanism ↗</a>	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	activities		

## Maintenance Tools

ID: FedRAMP Moderate MA-3 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Inspect Tools

ID: FedRAMP Moderate MA-3 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Inspect Media

ID: FedRAMP Moderate MA-3 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Prevent Unauthorized Removal

ID: FedRAMP Moderate MA-3 (3) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ a media sanitization mechanism ↗</a>	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Nonlocal Maintenance

ID: FedRAMP Moderate MA-4 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Document Nonlocal Maintenance

ID: FedRAMP Moderate MA-4 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Manage nonlocal maintenance and diagnostic activities ↗	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	1.1.0 ↗

## Maintenance Personnel

ID: FedRAMP Moderate MA-5 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Designate personnel to supervise unauthorized maintenance activities ↗	CMA_C1422 - Designate personnel to supervise unauthorized maintenance activities	Manual, Disabled	1.1.0 ↗
Maintain list of authorized remote maintenance personnel ↗	CMA_C1420 - Maintain list of authorized remote maintenance personnel	Manual, Disabled	1.1.0 ↗
Manage maintenance personnel ↗	CMA_C1421 - Manage maintenance personnel	Manual, Disabled	1.1.0 ↗

## Individuals Without Appropriate Access

ID: FedRAMP Moderate MA-5 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗

## Timely Maintenance

ID: FedRAMP Moderate MA-6 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide timely maintenance support ↗	CMA_C1425 - Provide timely maintenance support	Manual, Disabled	1.1.0 ↗

## Media Protection

### Media Protection Policy And Procedures

ID: FedRAMP Moderate MP-1 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update media protection policies and procedures ↗	CMA_C1427 - Review and update media protection policies and procedures	Manual, Disabled	1.1.0 ↗

## Media Access

ID: FedRAMP Moderate MP-2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure all media ↴	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Media Marking

ID: FedRAMP Moderate MP-3 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure all media ↴	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Media Storage

ID: FedRAMP Moderate MP-4 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↴	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Implement controls to secure all media ↴	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Media Transport

ID: FedRAMP Moderate MP-5 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure all media ↴	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗

## Cryptographic Protection

ID: FedRAMP Moderate MP-5 (4) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗

## Media Sanitization

ID: FedRAMP Moderate MP-6 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗

## Equipment Testing

ID: FedRAMP Moderate MP-6 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Media Use

ID: FedRAMP Moderate MP-7 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Restrict media use ↗	CMA_0450 - Restrict media use	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Prohibit Use Without Owner

ID: FedRAMP Moderate MP-7 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Restrict media use ↗</a>	CMA_0450 - Restrict media use	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Physical And Environmental Protection

### Physical And Environmental Protection Policy And Procedures

ID: FedRAMP Moderate PE-1 Ownership: Shared

[\[\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Review and update physical and environmental policies and procedures ↗</a>	CMA_C1446 - Review and update physical and environmental policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Physical Access Authorizations

ID: FedRAMP Moderate PE-2 Ownership: Shared

[\[\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Physical Access Control

ID: FedRAMP Moderate PE-3 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define a physical key management process ↗</a>	CMA_0115 - Define a physical key management process	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and maintain an asset inventory ↗</a>	CMA_0266 - Establish and maintain an asset inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Access Control For Transmission Medium

ID: FedRAMP Moderate PE-4 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Access Control For Output Devices

ID: FedRAMP Moderate PE-5 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and</a>	CMA_0323 - Implement physical security for offices, working areas,	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">secure areas ↗</a>	and secure areas		
<a href="#">Manage the input, output, processing, and storage of data ↗</a>	CMA_0369 - Manage the input, output, processing, and storage of data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Intrusion Alarms / Surveillance Equipment

ID: FedRAMP Moderate PE-6 (1) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Install an alarm system ↗</a>	CMA_0338 - Install an alarm system	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage a secure surveillance camera system ↗</a>	CMA_0354 - Manage a secure surveillance camera system	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Visitor Access Records

ID: FedRAMP Moderate PE-8 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Emergency Lighting

ID: FedRAMP Moderate PE-12 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ automatic emergency lighting ↗</a>	CMA_0209 - Employ automatic emergency lighting	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Fire Protection

ID: FedRAMP Moderate PE-13 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Suppression Devices / Systems

ID: FedRAMP Moderate PE-13 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automatic Fire Suppression

ID: FedRAMP Moderate PE-13 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Temperature And Humidity Controls

ID: FedRAMP Moderate PE-14 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Monitoring With Alarms / Notifications

ID: FedRAMP Moderate PE-14 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Install an alarm system ↗</a>	CMA_0338 - Install an alarm system	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Water Damage Protection

ID: FedRAMP Moderate PE-15 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	1.1.0 ↗

## Delivery And Removal

ID: FedRAMP Moderate PE-16 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define requirements for managing assets ↗	CMA_0125 - Define requirements for managing assets	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗

## Alternate Work Site

ID: FedRAMP Moderate PE-17 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure alternate work sites ↗	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	1.1.0 ↗

## Planning

### Security Planning Policy And Procedures

ID: FedRAMP Moderate PL-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update planning policies and procedures ↗	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	1.1.0 ↗

## System Security Plan

ID: FedRAMP Moderate PL-2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	1.1.0 ↗
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	1.1.0 ↗
Develop SSP that meets criteria ↗	CMA_C1492 - Develop SSP that meets criteria	Manual, Disabled	1.1.0 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	1.1.0 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗

## Plan / Coordinate With Other Organizational Entities

ID: FedRAMP Moderate PL-2 (3) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Rules Of Behavior

ID: FedRAMP Moderate PL-4 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop acceptable use policies and procedures ↗	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce rules of behavior and access agreements ↗	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Social Media And Networking Restrictions

ID: FedRAMP Moderate PL-4 (1) Ownership: Shared

[\[ \]](#) Expand table

Name	Description	Effect(s)	Version
(GitHub)			
Develop acceptable use policies and procedures ↗	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Information Security Architecture

ID: FedRAMP Moderate PL-8 Ownership: Shared

[\[ \]](#) Expand table

Name	Description	Effect(s)	Version
(GitHub)			
Develop a concept of operations (CONOPS) ↗	CMA_0141 - Develop a concept of operations (CONOPS)	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update the information security architecture ↗	CMA_C1504 - Review and update the information security architecture	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Personnel Security

## Personnel Security Policy And Procedures

ID: FedRAMP Moderate PS-1 Ownership: Shared

[\[ \]](#) Expand table

Name	Description	Effect(s)	Version
(GitHub)			
Review and update personnel security policies and procedures ↗	CMA_C1507 - Review and update personnel security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Position Risk Designation

ID: FedRAMP Moderate PS-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assign risk designations ↗</a>	CMA_0016 - Assign risk designations	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Personnel Screening

ID: FedRAMP Moderate PS-3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Clear personnel with access to classified information ↗</a>	CMA_0054 - Clear personnel with access to classified information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement personnel screening ↗</a>	CMA_0322 - Implement personnel screening	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Rescreen individuals at a defined frequency ↗</a>	CMA_C1512 - Rescreen individuals at a defined frequency	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information With Special Protection Measures

ID: FedRAMP Moderate PS-3 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Protect special information ↗</a>	CMA_0409 - Protect special information	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Personnel Termination

ID: FedRAMP Moderate PS-4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct exit interview upon termination ↗	CMA_0058 - Conduct exit interview upon termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify upon termination or transfer ↗	CMA_0381 - Notify upon termination or transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect against and prevent data theft from departing employees ↗	CMA_0398 - Protect against and prevent data theft from departing employees	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Personnel Transfer

ID: FedRAMP Moderate PS-5 Ownership: Shared

[ ] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Initiate transfer or reassignment actions ↗	CMA_0333 - Initiate transfer or reassignment actions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Modify access authorizations upon personnel transfer ↗	CMA_0374 - Modify access authorizations upon personnel transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify upon termination or transfer ↗	CMA_0381 - Notify upon termination or transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Reevaluate access upon personnel transfer ↗	CMA_0424 - Reevaluate access upon personnel transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Access Agreements

ID: FedRAMP Moderate PS-6 Ownership: Shared

[ ] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document organizational access agreements ↗	CMA_0192 - Document organizational access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce rules of behavior and access agreements ↗	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Ensure access agreements are signed or resigned timely ↗	CMA_C1528 - Ensure access agreements are signed or resigned timely	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require users to sign access agreement ↗	CMA_0440 - Require users to sign access agreement	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update organizational access agreements ↗	CMA_0520 - Update organizational access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Third-Party Personnel Security

ID: FedRAMP Moderate PS-7 Ownership: Shared

[+] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document third-party personnel security requirements ↗	CMA_C1531 - Document third-party personnel security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require notification of third-party personnel transfer or termination ↗	CMA_C1532 - Require notification of third-party personnel transfer or termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require third-party providers to comply with personnel security policies and procedures ↗	CMA_C1530 - Require third-party providers to comply with personnel security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Personnel Sanctions

ID: FedRAMP Moderate PS-8 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement formal sanctions process ↗	CMA_0317 - Implement formal sanctions process	Manual, Disabled	1.1.0 ↗
Notify personnel upon sanctions ↗	CMA_0380 - Notify personnel upon sanctions	Manual, Disabled	1.1.0 ↗

## Risk Assessment

### Risk Assessment Policy And Procedures

ID: FedRAMP Moderate RA-1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update risk assessment policies and procedures ↗	CMA_C1537 - Review and update risk assessment policies and procedures	Manual, Disabled	1.1.0 ↗

## Security Categorization

ID: FedRAMP Moderate RA-2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Categorize information ↗	CMA_0052 - Categorize information	Manual, Disabled	1.1.0 ↗
Develop business classification schemes ↗	CMA_0155 - Develop business classification schemes	Manual, Disabled	1.1.0 ↗
Ensure security categorization is approved ↗	CMA_C1540 - Ensure security categorization is approved	Manual, Disabled	1.1.0 ↗
Review label activity and	CMA_0474 - Review label activity and	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">analytics ↗</a>	analytics	Disabled	

## Risk Assessment

ID: FedRAMP Moderate RA-3 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Conduct Risk Assessment ↗</a>	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct risk assessment and distribute its results ↗</a>	CMA_C1544 - Conduct risk assessment and distribute its results	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct risk assessment and document its results ↗</a>	CMA_C1542 - Conduct risk assessment and document its results	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a risk assessment ↗</a>	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Vulnerability Scanning

ID: FedRAMP Moderate RA-5 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">A vulnerability assessment solution should be enabled on your virtual machines ↗</a>	Audits virtual machines to detect whether they are running a supported vulnerability assessment solution. A core component of every cyber risk and security program is the identification and analysis of vulnerabilities. Azure Security Center's standard pricing tier includes vulnerability scanning for your virtual machines at no extra cost. Additionally, Security Center can automatically deploy this tool for you.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

<b>Name</b>  (Azure portal)	<b>Description</b>	<b>Effect(s)</b>  (GitHub)	<b>Version</b>
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Resource Manager should be enabled ↗</a>	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for servers should be enabled ↗</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for SQL servers on machines should be enabled ↴	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↴	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↴	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Container registry images should have vulnerability findings resolved ↴	Container image vulnerability assessment scans your registry for security vulnerabilities and exposes detailed findings for each image.  Resolving the vulnerabilities can greatly improve your containers' security posture and protect them from attacks.	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
Microsoft Defender for Containers should be enabled ↴	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
Microsoft Defender for Storage should be enabled ↴	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption.  The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
Perform vulnerability scans ↴	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Remediate information	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">system flaws ↗</a>			
<a href="#">SQL databases should have vulnerability findings resolved ↗</a>	Monitor vulnerability assessment scan results and recommendations for how to remediate database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">4.1.0 ↗</a>
<a href="#">SQL servers on machines should have vulnerability findings resolved ↗</a>	SQL vulnerability assessment scans your database for security vulnerabilities, and exposes any deviations from best practices such as misconfigurations, excessive permissions, and unprotected sensitive data. Resolving the vulnerabilities found can greatly improve your database security posture.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Vulnerabilities in container security configurations should be remediated ↗</a>	Audit vulnerabilities in security configuration on machines with Docker installed and display as recommendations in Azure Security Center.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Vulnerabilities in security configuration on your machines should be remediated ↗</a>	Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
<a href="#">Vulnerabilities in security configuration on your virtual machine scale sets should be remediated ↗</a>	Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Vulnerability assessment should be enabled on SQL Managed Instance ↗</a>	Audit each SQL Managed Instance which doesn't have recurring vulnerability assessment scans enabled. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Vulnerability assessment should be enabled on your SQL servers ↗</a>	Audit Azure SQL servers which do not have vulnerability assessment properly configured. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Vulnerability assessment should be enabled on your Synapse workspaces ↗	Discover, track, and remediate potential vulnerabilities by configuring recurring SQL vulnerability assessment scans on your Synapse workspaces.	AuditIfNotExists, Disabled	1.0.0 ↗

## Update Tool Capability

ID: FedRAMP Moderate RA-5 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗

## Update By Frequency / Prior To New Scan / When Identified

ID: FedRAMP Moderate RA-5 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗

## Breadth / Depth Of Coverage

ID: FedRAMP Moderate RA-5 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Perform vulnerability scans ↗</a>	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Privileged Access

ID: FedRAMP Moderate RA-5 (5) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement privileged access for executing vulnerability scanning activities ↗</a>	CMA_C1555 - Implement privileged access for executing vulnerability scanning activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Trend Analyses

ID: FedRAMP Moderate RA-5 (6) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Observe and report security weaknesses ↗</a>	CMA_0384 - Observe and report security weaknesses	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a trend analysis on threats ↗</a>	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform threat modeling ↗</a>	CMA_0392 - Perform threat modeling	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform vulnerability scans ↗</a>	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Review Historic Audit Logs

ID: FedRAMP Moderate RA-5 (8) Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit privileged functions ↗</a>	CMA_0019 - Audit privileged functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Correlate audit records ↗</a>	CMA_0087 - Correlate audit records	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Determine auditable events ↗</a>	CMA_0137 - Determine auditable events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish requirements for audit review and reporting ↗</a>	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Integrate audit review, analysis, and reporting ↗</a>	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Integrate cloud app security with a siem ↗</a>	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review account provisioning logs ↗</a>	CMA_0460 - Review account provisioning logs	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review administrator assignments weekly ↗</a>	CMA_0461 - Review administrator assignments weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review audit data ↗</a>	CMA_0466 - Review audit data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review cloud identity report overview ↗</a>	CMA_0468 - Review cloud identity report overview	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review controlled folder access events ↗</a>	CMA_0471 - Review controlled folder access events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review exploit protection events ↗</a>	CMA_0472 - Review exploit protection events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review file and folder activity ↗</a>	CMA_0473 - Review file and folder activity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review role group changes weekly ↗	CMA_0476 - Review role group changes weekly	Manual, Disabled	1.1.0 ↗

# System And Services Acquisition

## System And Services Acquisition Policy And Procedures

ID: FedRAMP Moderate SA-1 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update system and services acquisition policies and procedures ↗	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	1.1.0 ↗

# Allocation Of Resources

ID: FedRAMP Moderate SA-2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Align business objectives and IT goals ↗	CMA_0008 - Align business objectives and IT goals	Manual, Disabled	1.1.0 ↗
Allocate resources in determining information system requirements ↗	CMA_C1561 - Allocate resources in determining information system requirements	Manual, Disabled	1.1.0 ↗
Establish a discrete line item in budgeting documentation ↗	CMA_C1563 - Establish a discrete line item in budgeting documentation	Manual, Disabled	1.1.0 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Govern the allocation of resources ↗	CMA_0293 - Govern the allocation of resources	Manual, Disabled	1.1.0 ↗
Secure commitment from leadership ↗	CMA_0489 - Secure commitment from leadership	Manual, Disabled	1.1.0 ↗

## System Development Life Cycle

ID: FedRAMP Moderate SA-3 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define information security roles and responsibilities ↗	CMA_C1565 - Define information security roles and responsibilities	Manual, Disabled	1.1.0 ↗
Identify individuals with security roles and responsibilities ↗	CMA_C1566 - Identify individuals with security roles and responsibilities	Manual, Disabled	1.1.1 ↗
Integrate risk management process into SDLC ↗	CMA_C1567 - Integrate risk management process into SDLC	Manual, Disabled	1.1.0 ↗

## Acquisition Process

ID: FedRAMP Moderate SA-4 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Determine supplier contract obligations ↗	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	1.1.0 ↗
Document acquisition contract acceptance criteria ↗	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	1.1.0 ↗
Document protection of personal data in acquisition contracts ↗	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document protection of security information in acquisition contracts ↗	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document requirements for the use of shared data in contracts ↗	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	1.1.0 ↗
Document security assurance requirements in acquisition contracts ↗	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document security documentation requirements in acquisition contract ↗	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	1.1.0 ↗
Document security functional requirements in acquisition contracts ↗	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the protection of cardholder data in third party contracts ↗	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	1.1.0 ↗

## Functional Properties Of Security Controls

ID: FedRAMP Moderate SA-4 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Obtain functional properties of security controls ↗	CMA_C1575 - Obtain functional properties of security controls	Manual, Disabled	1.1.0 ↗

# Design / Implementation Information For Security Controls

ID: FedRAMP Moderate SA-4 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Obtain design and implementation information for the security controls ↴	CMA_C1576 - Obtain design and implementation information for the security controls	Manual, Disabled	<a href="#">1.1.1 ↴</a>

# Continuous Monitoring Plan

ID: FedRAMP Moderate SA-4 (8) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Obtain continuous monitoring plan for security controls ↴	CMA_C1577 - Obtain continuous monitoring plan for security controls	Manual, Disabled	<a href="#">1.1.0 ↴</a>

# Functions / Ports / Protocols / Services In Use

ID: FedRAMP Moderate SA-4 (9) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require developer to identify SDLC ports, protocols, and services ↴	CMA_C1578 - Require developer to identify SDLC ports, protocols, and services	Manual, Disabled	<a href="#">1.1.0 ↴</a>

# Use Of Approved Piv Products

ID: FedRAMP Moderate SA-4 (10) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ FIPS 201-approved technology for PIV ↗</a>	CMA_C1579 - Employ FIPS 201-approved technology for PIV	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information System Documentation

ID: FedRAMP Moderate SA-5 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Distribute information system documentation ↗</a>	CMA_C1584 - Distribute information system documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document customer-defined actions ↗</a>	CMA_C1582 - Document customer-defined actions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Obtain Admin documentation ↗</a>	CMA_C1580 - Obtain Admin documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Obtain user security function documentation ↗</a>	CMA_C1581 - Obtain user security function documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Protect administrator and user documentation ↗</a>	CMA_C1583 - Protect administrator and user documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## External Information System Services

ID: FedRAMP Moderate SA-9 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define and document government oversight ↗</a>	CMA_C1587 - Define and document government oversight	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require external service providers to comply with security requirements ↗</a>	CMA_C1586 - Require external service providers to comply with security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review cloud service provider's compliance with policies and agreements ↗	CMA_0469 - Review cloud service provider's compliance with policies and agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Risk Assessments / Organizational Approvals

ID: FedRAMP Moderate SA-9 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess risk in third party relationships ↗	CMA_0014 - Assess risk in third party relationships	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Obtain approvals for acquisitions and outsourcing ↗	CMA_C1590 - Obtain approvals for acquisitions and outsourcing	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Identification Of Functions / Ports / Protocols / Services

ID: FedRAMP Moderate SA-9 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Identify external service providers ↗	CMA_C1591 - Identify external service providers	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Consistent Interests Of Consumers And Providers

ID: FedRAMP Moderate SA-9 (4) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure external providers consistently meet interests of the customers ↴	CMA_C1592 - Ensure external providers consistently meet interests of the customers	Manual, Disabled	1.1.0 ↴

## Processing, Storage, And Service Location

ID: FedRAMP Moderate SA-9 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Restrict location of information processing, storage and services ↴	CMA_C1593 - Restrict location of information processing, storage and services	Manual, Disabled	1.1.0 ↴

## Developer Configuration Management

ID: FedRAMP Moderate SA-10 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Address coding vulnerabilities ↴	CMA_0003 - Address coding vulnerabilities	Manual, Disabled	1.1.0 ↴
Develop and document application security requirements ↴	CMA_0148 - Develop and document application security requirements	Manual, Disabled	1.1.0 ↴
Document the information system environment in acquisition contracts ↴	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↴
Establish a secure software development program ↴	CMA_0259 - Establish a secure software development program	Manual, Disabled	1.1.0 ↴
Perform vulnerability scans ↴	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↴
Remediate information system	CMA_0427 - Remediate information	Manual,	1.1.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">flaws ↗</a>	system flaws	Disabled	
<a href="#">Require developers to document approved changes and potential impact ↗</a>	CMA_C1597 - Require developers to document approved changes and potential impact	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require developers to implement only approved changes ↗</a>	CMA_C1596 - Require developers to implement only approved changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require developers to manage change integrity ↗</a>	CMA_C1595 - Require developers to manage change integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Software / Firmware Integrity Verification

ID: FedRAMP Moderate SA-10 (1) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Verify software, firmware and information integrity ↗</a>	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Developer Security Testing And Evaluation

ID: FedRAMP Moderate SA-11 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Perform vulnerability scans ↗</a>	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require developers to produce evidence of security assessment plan execution ↗</a>	CMA_C1602 - Require developers to produce evidence of security assessment plan execution	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# System And Communications Protection

## System And Communications Protection Policy And Procedures

ID: FedRAMP Moderate SC-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update system and communications protection policies and procedures ↗</a>	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Application Partitioning

ID: FedRAMP Moderate SC-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authorize remote access ↗</a>	CMA_0024 - Authorize remote access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Separate user and information system management functionality ↗</a>	CMA_0493 - Separate user and information system management functionality	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Use dedicated machines for administrative tasks ↗</a>	CMA_0527 - Use dedicated machines for administrative tasks	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Denial Of Service Protection

ID: FedRAMP Moderate SC-5 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure DDoS Protection Standard should be enabled ↗	DDoS protection standard should be enabled for all virtual networks with a subnet that is part of an application gateway with a public IP.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Azure Web Application Firewall should be enabled for Azure Front Door entry-points ↗	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.	Audit, Deny, Disabled	<a href="#">1.0.2 ↗</a>
Develop and document a DDoS response plan ↗	CMA_0147 - Develop and document a DDoS response plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
IP Forwarding on your virtual machine should be disabled ↗	Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely required (e.g., when using the VM as a network virtual appliance), and therefore, this should be reviewed by the network security team.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Web Application Firewall (WAF) should be enabled for Application Gateway ↗	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>

## Resource Availability

ID: FedRAMP Moderate SC-6 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Govern the allocation of resources ↗	CMA_0293 - Govern the allocation of resources	Manual, Disabled	1.1.0 ↗
Manage availability and capacity ↗	CMA_0356 - Manage availability and capacity	Manual, Disabled	1.1.0 ↗
Secure commitment from leadership ↗	CMA_0489 - Secure commitment from leadership	Manual, Disabled	1.1.0 ↗

## Boundary Protection

ID: FedRAMP Moderate SC-7 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: All Internet traffic should be routed via your deployed Azure Firewall ↗	Azure Security Center has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall	AuditIfNotExists, Disabled	3.0.0-preview ↗
[Preview]: Storage account public access should be disallowed ↗	Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it.	audit, Audit, deny, Deny, disabled, Disabled	3.1.0-preview ↗
Adaptive network hardening recommendations should be applied on internet facing virtual machines ↗	Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface	AuditIfNotExists, Disabled	3.0.0 ↗
All network ports should be	Azure Security Center has identified some of your network security groups' inbound	AuditIfNotExists, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
restricted on network security groups associated to your virtual machine ↗	rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.		
API Management services should use a virtual network ↗	Azure Virtual Network deployment provides enhanced security, isolation and allows you to place your API Management service in a non-internet routable network that you control access to. These networks can then be connected to your on-premises networks using various VPN technologies, which enables access to your backend services within the network and/or on-premises. The developer portal and API gateway, can be configured to be accessible either from the Internet or only within the virtual network.	Audit, Deny, Disabled	1.0.2 ↗
App Configuration should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> ↗ .	AuditIfNotExists, Disabled	1.0.2 ↗
Authorized IP ranges should be defined on Kubernetes Services ↗	Restrict access to the Kubernetes Service Management API by granting API access only to IP addresses in specific ranges. It is recommended to limit access to authorized IP ranges to ensure that only applications from allowed networks can access the cluster.	Audit, Disabled	2.0.1 ↗
Azure API for FHIR should use private link ↗	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> .		
Azure Cache for Redis should use private link ↗	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Cognitive Search service should use a SKU that supports private link ↗	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should disable public network access ↗	Disabling public network access improves security by ensuring that your Azure Cognitive Search service is not exposed on the public internet. Creating private endpoints can limit exposure of your Search service. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Cosmos DB accounts should have firewall rules ↴	<p>Firewall rules should be defined on your Azure Cosmos DB accounts to prevent traffic from unauthorized sources.</p> <p>Accounts that have at least one IP rule defined with the virtual network filter enabled are deemed compliant. Accounts disabling public access are also deemed compliant.</p>	Audit, Deny, Disabled	2.0.0 ↴
Azure Data Factory should use private link ↴	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a>.</p>	AuditIfNotExists, Disabled	1.0.0 ↴
Azure Event Grid domains should use private link ↴	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> .</p>	Audit, Disabled	1.0.2 ↴
Azure Event Grid topics should use private link ↴	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn</p>	Audit, Disabled	1.0.2 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints ↗</a> .		
Azure File Sync should use private link ↗	Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Key Vault should have firewall enabled ↗	Enable the key vault firewall so that the key vault is not accessible by default to any public IPs. Optionally, you can configure specific IP ranges to limit access to those networks. Learn more at: <a href="https://docs.microsoft.com/azure/key-vault/general/network-security">https://docs.microsoft.com/azure/key-vault/general/network-security</a>	Audit, Deny, Disabled	3.2.1 ↗
Azure Key Vaults should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink ↗</a> .	[parameters('audit_effect')]	1.2.1 ↗
Azure Machine Learning workspaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .	Audit, Disabled	1.0.0 ↗
Azure Service Bus namespaces	Azure Private Link lets you connect your virtual network to Azure services without a	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should use private link ↗</a>	public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .		
<a href="#">Azure SignalR Service should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .	Audit, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Synapse workspaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a> .	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Azure Web Application Firewall should be enabled for Azure Front Door entry-points ↗</a>	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by	Audit, Deny, Disabled	<a href="#">1.0.2 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	countries, IP address ranges, and other http(s) parameters via custom rules.		
Azure Web PubSub Service should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a> ↗ .	Audit, Disabled	1.0.0 ↗
Cognitive Services accounts should disable public network access ↗	To improve the security of Cognitive Services accounts, ensure that it isn't exposed to the public internet and can only be accessed from a private endpoint. Disable the public network access property as described in <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> ↗ . This option disables access from any public address space outside the Azure IP range, and denies all logins that match IP or virtual network-based firewall rules. This reduces data leakage risks.	Audit, Deny, Disabled	3.0.1 ↗
Cognitive Services accounts should restrict network access ↗	Network access to Cognitive Services accounts should be restricted. Configure network rules so only applications from allowed networks can access the Cognitive Services account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges.	Audit, Deny, Disabled	3.0.0 ↗
Cognitive Services should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll	Audit, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>reduce the potential for data leakage.</p> <p>Learn more about private links at: <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a>.</p>		
<a href="#">Container registries should not allow unrestricted network access ↗</a>	<p>Azure container registries by default accept connections over the internet from hosts on any network. To protect your registries from potential threats, allow access from only specific private endpoints, public IP addresses or address ranges. If your registry doesn't have network rules configured, it will appear in the unhealthy resources. Learn more about Container Registry network rules here:</p> <p><a href="https://aka.ms/acr/privatelink">https://aka.ms/acr/privatelink</a>,  <a href="https://aka.ms/acr/portal/public-network">https://aka.ms/acr/portal/public-network</a> and <a href="https://aka.ms/acr/vnet">https://aka.ms/acr/vnet</a>.</p>	Audit, Deny, Disabled	2.0.0 ↗
<a href="#">Container registries should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a>.</p>	Audit, Disabled	1.0.1 ↗
<a href="#">CosmosDB accounts should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at:</p> <p><a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a>.</p>	Audit, Disabled	1.0.0 ↗
<a href="#">Disk access resources should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or</p>	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a>.</p>		
<a href="#">Event Hub namespaces should use private link</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a>.</p>	AuditIfNotExists, Disabled	1.0.0 <a href="#">↗</a>
<a href="#">Implement system boundary protection</a>	CMA_0328 - Implement system boundary protection	Manual, Disabled	1.1.0 <a href="#">↗</a>
<a href="#">Internet-facing virtual machines should be protected with network security groups</a>	<p>Protect your virtual machines from potential threats by restricting access to them with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/ng-doc">https://aka.ms/ng-doc</a></p>	AuditIfNotExists, Disabled	3.0.0 <a href="#">↗</a>
<a href="#">IoT Hub device provisioning service instances should use private link</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a>.</p>	Audit, Disabled	1.0.0 <a href="#">↗</a>
<a href="#">IP Forwarding on your virtual machine should be disabled</a>	Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely	AuditIfNotExists, Disabled	3.0.0 <a href="#">↗</a>

Name (Azure portal)	Description(s) .., when using the VM as a network virtual appliance), and therefore, this should be reviewed by the network security team.	Effect(s)	Version (GitHub)
Management ports of virtual machines should be protected with just-in-time network access control ↴	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.0.0 ↴
Management ports should be closed on your virtual machines ↴	Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine.	AuditIfNotExists, Disabled	3.0.0 ↴
Non-internet-facing virtual machines should be protected with network security groups ↴	Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsg-doc">https://aka.ms/nsg-doc</a> ↴	AuditIfNotExists, Disabled	3.0.0 ↴
Private endpoint connections on Azure SQL Database should be enabled ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↴
Private endpoint should be enabled for MariaDB servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↴
Private endpoint should be enabled for MySQL servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Private endpoint should be enabled for PostgreSQL servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↴
Public network access on Azure SQL Database should be disabled ↴	Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP or virtual network based firewall rules.	Audit, Deny, Disabled	1.1.0 ↴
Public network access should be disabled for MariaDB servers ↴	Disable the public network access property to improve security and ensure your Azure Database for MariaDB can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↴
Public network access should be disabled for MySQL servers ↴	Disable the public network access property to improve security and ensure your Azure Database for MySQL can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↴
Public network access should be disabled for PostgreSQL servers ↴	Disable the public network access property to improve security and ensure your Azure Database for PostgreSQL can only be accessed from a private endpoint. This configuration disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.1 ↴
Storage accounts should restrict network access ↴	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow	Audit, Deny, Disabled	1.1.1 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges		
<a href="#">Storage accounts should restrict network access using virtual network rules ↗</a>	Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.	Audit, Deny, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Storage accounts should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview ↗</a>	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Subnets should be associated with a Network Security Group ↗</a>	Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">VM Image Builder templates should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .	Audit, Disabled, Deny	<a href="#">1.1.0 ↗</a>
<a href="#">Web Application Firewall (WAF) should be</a>	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">enabled for Application Gateway ↗</a>	incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.		

## Access Points

ID: FedRAMP Moderate SC-7 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Preview]: All Internet traffic should be routed via your deployed Azure Firewall ↗</a>	Azure Security Center has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall	AuditIfNotExists, Disabled	<a href="#">3.0.0-preview ↗</a>
<a href="#">[Preview]: Storage account public access should be disallowed ↗</a>	Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it.	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">3.1.0-preview ↗</a>
<a href="#">Adaptive network hardening recommendations should be applied on internet facing virtual machines ↗</a>	Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">All network ports should be restricted on</a>	Azure Security Center has identified some of your network security groups' inbound rules to be too permissive. Inbound rules	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">network security groups associated to your virtual machine ↗</a>	should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.		
<a href="#">API Management services should use a virtual network ↗</a>	Azure Virtual Network deployment provides enhanced security, isolation and allows you to place your API Management service in a non-internet routable network that you control access to. These networks can then be connected to your on-premises networks using various VPN technologies, which enables access to your backend services within the network and/or on-premises. The developer portal and API gateway, can be configured to be accessible either from the Internet or only within the virtual network.	Audit, Deny, Disabled	1.0.2 ↗
<a href="#">App Configuration should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> ↗ .	AuditIfNotExists, Disabled	1.0.2 ↗
<a href="#">Authorized IP ranges should be defined on Kubernetes Services ↗</a>	Restrict access to the Kubernetes Service Management API by granting API access only to IP addresses in specific ranges. It is recommended to limit access to authorized IP ranges to ensure that only applications from allowed networks can access the cluster.	Audit, Disabled	2.0.1 ↗
<a href="#">Azure API for FHIR should use private link ↗</a>	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> .		
Azure Cache for Redis should use private link ↗	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Cognitive Search service should use a SKU that supports private link ↗	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should disable public network access ↗	Disabling public network access improves security by ensuring that your Azure Cognitive Search service is not exposed on the public internet. Creating private endpoints can limit exposure of your Search service. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Cosmos DB accounts should have firewall rules ↴	<p>Firewall rules should be defined on your Azure Cosmos DB accounts to prevent traffic from unauthorized sources.</p> <p>Accounts that have at least one IP rule defined with the virtual network filter enabled are deemed compliant. Accounts disabling public access are also deemed compliant.</p>	Audit, Deny, Disabled	2.0.0 ↴
Azure Data Factory should use private link ↴	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a>.</p>	AuditIfNotExists, Disabled	1.0.0 ↴
Azure Event Grid domains should use private link ↴	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> .</p>	Audit, Disabled	1.0.2 ↴
Azure Event Grid topics should use private link ↴	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn</p>	Audit, Disabled	1.0.2 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints ↗</a> .		
Azure File Sync should use private link ↗	Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Key Vault should have firewall enabled ↗	Enable the key vault firewall so that the key vault is not accessible by default to any public IPs. Optionally, you can configure specific IP ranges to limit access to those networks. Learn more at: <a href="https://docs.microsoft.com/azure/key-vault/general/network-security">https://docs.microsoft.com/azure/key-vault/general/network-security</a>	Audit, Deny, Disabled	3.2.1 ↗
Azure Key Vaults should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink ↗</a> .	[parameters('audit_effect')]	1.2.1 ↗
Azure Machine Learning workspaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .	Audit, Disabled	1.0.0 ↗
Azure Service Bus namespaces	Azure Private Link lets you connect your virtual network to Azure services without a	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should use private link ↗</a>	public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .		
<a href="#">Azure SignalR Service should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .	Audit, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Synapse workspaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a> .	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Azure Web Application Firewall should be enabled for Azure Front Door entry-points ↗</a>	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by	Audit, Deny, Disabled	<a href="#">1.0.2 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	countries, IP address ranges, and other http(s) parameters via custom rules.		
Azure Web PubSub Service should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a> ↗ .	Audit, Disabled	1.0.0 ↗
Cognitive Services accounts should disable public network access ↗	To improve the security of Cognitive Services accounts, ensure that it isn't exposed to the public internet and can only be accessed from a private endpoint. Disable the public network access property as described in <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> ↗ . This option disables access from any public address space outside the Azure IP range, and denies all logins that match IP or virtual network-based firewall rules. This reduces data leakage risks.	Audit, Deny, Disabled	3.0.1 ↗
Cognitive Services accounts should restrict network access ↗	Network access to Cognitive Services accounts should be restricted. Configure network rules so only applications from allowed networks can access the Cognitive Services account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges.	Audit, Deny, Disabled	3.0.0 ↗
Cognitive Services should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll	Audit, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>reduce the potential for data leakage.</p> <p>Learn more about private links at: <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a>.</p>		
<a href="#">Container registries should not allow unrestricted network access ↗</a>	<p>Azure container registries by default accept connections over the internet from hosts on any network. To protect your registries from potential threats, allow access from only specific private endpoints, public IP addresses or address ranges. If your registry doesn't have network rules configured, it will appear in the unhealthy resources. Learn more about Container Registry network rules here:</p> <p><a href="https://aka.ms/acr/privatelink">https://aka.ms/acr/privatelink</a>,  <a href="https://aka.ms/acr/portal/public-network">https://aka.ms/acr/portal/public-network</a> and <a href="https://aka.ms/acr/vnet">https://aka.ms/acr/vnet</a>.</p>	Audit, Deny, Disabled	2.0.0 ↗
<a href="#">Container registries should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a>.</p>	Audit, Disabled	1.0.1 ↗
<a href="#">CosmosDB accounts should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at:</p> <p><a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a>.</p>	Audit, Disabled	1.0.0 ↗
<a href="#">Disk access resources should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or</p>	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a>.</p>		
<a href="#">Event Hub namespaces should use private link</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a>.</p>	AuditIfNotExists, Disabled	1.0.0 <a href="#">↗</a>
<a href="#">Internet-facing virtual machines should be protected with network security groups</a>	<p>Protect your virtual machines from potential threats by restricting access to them with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsg-doc">https://aka.ms/nsg-doc</a>.</p>	AuditIfNotExists, Disabled	3.0.0 <a href="#">↗</a>
<a href="#">IoT Hub device provisioning service instances should use private link</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a>.</p>	Audit, Disabled	1.0.0 <a href="#">↗</a>
<a href="#">IP Forwarding on your virtual machine should be disabled</a>	<p>Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely required (e.g., when using the VM as a network virtual appliance), and therefore,</p>	AuditIfNotExists, Disabled	3.0.0 <a href="#">↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	this should be reviewed by the network security team.		
Management ports of virtual machines should be protected with just-in-time network access control ↗	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.0.0 ↗
Management ports should be closed on your virtual machines ↗	Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine.	AuditIfNotExists, Disabled	3.0.0 ↗
Non-internet-facing virtual machines should be protected with network security groups ↗	Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsq-doc">https://aka.ms/nsq-doc</a> ↗	AuditIfNotExists, Disabled	3.0.0 ↗
Private endpoint connections on Azure SQL Database should be enabled ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↗
Private endpoint should be enabled for MariaDB servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for MySQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Private endpoint should be enabled for PostgreSQL servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↴
Public network access on Azure SQL Database should be disabled ↴	Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP or virtual network based firewall rules.	Audit, Deny, Disabled	1.1.0 ↴
Public network access should be disabled for MariaDB servers ↴	Disable the public network access property to improve security and ensure your Azure Database for MariaDB can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↴
Public network access should be disabled for MySQL servers ↴	Disable the public network access property to improve security and ensure your Azure Database for MySQL can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↴
Public network access should be disabled for PostgreSQL servers ↴	Disable the public network access property to improve security and ensure your Azure Database for PostgreSQL can only be accessed from a private endpoint. This configuration disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.1 ↴
Storage accounts should restrict network access ↴	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow	Audit, Deny, Disabled	1.1.1 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges		
<a href="#">Storage accounts should restrict network access using virtual network rules ↗</a>	Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.	Audit, Deny, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Storage accounts should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview ↗</a>	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Subnets should be associated with a Network Security Group ↗</a>	Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">VM Image Builder templates should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .	Audit, Disabled, Deny	<a href="#">1.1.0 ↗</a>
<a href="#">Web Application Firewall (WAF) should be</a>	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">enabled for Application Gateway ↗</a>	incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.		

## External Telecommunications Services

ID: FedRAMP Moderate SC-7 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement managed interface for each external service ↗</a>	CMA_C1626 - Implement managed interface for each external service	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement system boundary protection ↗</a>	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Secure the interface to external systems ↗</a>	CMA_0491 - Secure the interface to external systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Prevent Split Tunneling For Remote Devices

ID: FedRAMP Moderate SC-7 (7) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Prevent split tunneling for remote devices ↗</a>	CMA_C1632 - Prevent split tunneling for remote devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Route Traffic To Authenticated Proxy Servers

ID: FedRAMP Moderate SC-7 (8) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Route traffic through authenticated proxy network ↴	CMA_C1633 - Route traffic through authenticated proxy network	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Host-Based Protection

ID: FedRAMP Moderate SC-7 (12) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement system boundary protection ↴	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Isolation Of Security Tools / Mechanisms / Support Components

ID: FedRAMP Moderate SC-7 (13) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Isolate SecurID systems, Security Incident Management systems ↴	CMA_C1636 - Isolate SecurID systems, Security Incident Management systems	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Fail Secure

ID: FedRAMP Moderate SC-7 (18) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement system boundary protection ↴	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Manage transfers between standby and active system components ↴	CMA_0371 - Manage transfers between standby and active system components	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Transmission Confidentiality And Integrity

ID: FedRAMP Moderate SC-8 Ownership: Shared

[+] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">App Service apps should only be accessible over HTTPS ↴</a>	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	<a href="#">4.0.0 ↴</a>
<a href="#">App Service apps should require FTPS only ↴</a>	Enable FTPS enforcement for enhanced security.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>
<a href="#">App Service apps should use the latest TLS version ↴</a>	Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the latest TLS version for App Service apps to take advantage of security fixes, if any, and/or new functionalities of the latest version.	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↴</a>
<a href="#">Azure HDInsight clusters should use encryption in transit to encrypt communication between Azure HDInsight cluster nodes ↴</a>	Data can be tampered with during transmission between Azure HDInsight cluster nodes. Enabling encryption in transit addresses problems of misuse and tampering during this transmission.	Audit, Deny, Disabled	<a href="#">1.0.0 ↴</a>
<a href="#">Enforce SSL connection should be enabled for</a>	Azure Database for MySQL supports connecting your Azure Database for MySQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL	Audit, Disabled	<a href="#">1.0.1 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">MySQL database servers</a> ↗	connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration enforces that SSL is always enabled for accessing your database server.		
<a href="#">Enforce SSL connection should be enabled for PostgreSQL database servers</a> ↗	Azure Database for PostgreSQL supports connecting your Azure Database for PostgreSQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration enforces that SSL is always enabled for accessing your database server.	Audit, Disabled	<a href="#">1.0.1</a> ↗
<a href="#">Function apps should only be accessible over HTTPS</a> ↗	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	<a href="#">5.0.0</a> ↗
<a href="#">Function apps should require FTPS only</a> ↗	Enable FTPS enforcement for enhanced security.	AuditIfNotExists, Disabled	<a href="#">3.0.0</a> ↗
<a href="#">Function apps should use the latest TLS version</a> ↗	Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the latest TLS version for Function apps to take advantage of security fixes, if any, and/or new functionalities of the latest version.	AuditIfNotExists, Disabled	<a href="#">2.0.1</a> ↗
<a href="#">Kubernetes clusters should be accessible only over HTTPS</a> ↗	Use of HTTPS ensures authentication and protects data in transit from network layer eavesdropping attacks. This capability is currently generally available for Kubernetes Service (AKS), and in preview for Azure Arc enabled Kubernetes. For more info, visit <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> ↗	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">8.1.0</a> ↗
<a href="#">Only secure connections to your Azure Cache</a>	Audit enabling of only connections via SSL to Azure Cache for Redis. Use of secure connections ensures authentication between	Audit, Deny, Disabled	<a href="#">1.0.0</a> ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
for Redis should be enabled ↴	the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking		
Protect data in transit using encryption ↴	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↴
Protect passwords with encryption ↴	CMA_0408 - Protect passwords with encryption	Manual, Disabled	1.1.0 ↴
Secure transfer to storage accounts should be enabled ↴	Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking	Audit, Deny, Disabled	2.0.0 ↴
Windows machines should be configured to use secure communication protocols ↴	To protect the privacy of information communicated over the Internet, your machines should use the latest version of the industry-standard cryptographic protocol, Transport Layer Security (TLS). TLS secures communications over a network by encrypting a connection between machines.	AuditIfNotExists, Disabled	4.1.1 ↴

## Cryptographic Or Alternate Physical Protection

ID: FedRAMP Moderate SC-8 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
App Service apps should only be accessible over HTTPS ↴	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	4.0.0 ↴
App Service apps should require	Enable FTPS enforcement for enhanced security.	AuditIfNotExists, Disabled	3.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<b>FTPS only ↗</b>			
<a href="#">App Service apps should use the latest TLS version ↗</a>	Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the latest TLS version for App Service apps to take advantage of security fixes, if any, and/or new functionalities of the latest version.	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Azure HDInsight clusters should use encryption in transit to encrypt communication between Azure HDInsight cluster nodes ↗</a>	Data can be tampered with during transmission between Azure HDInsight cluster nodes. Enabling encryption in transit addresses problems of misuse and tampering during this transmission.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Configure workstations to check for digital certificates ↗</a>	CMA_0073 - Configure workstations to check for digital certificates	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce SSL connection should be enabled for MySQL database servers ↗</a>	Azure Database for MySQL supports connecting your Azure Database for MySQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration enforces that SSL is always enabled for accessing your database server.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Enforce SSL connection should be enabled for PostgreSQL database servers ↗</a>	Azure Database for PostgreSQL supports connecting your Azure Database for PostgreSQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This configuration enforces that SSL is always enabled for accessing your database server.	Audit, Disabled	<a href="#">1.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Function apps should only be accessible over HTTPS ↴	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	<a href="#">5.0.0 ↴</a>
Function apps should require FTPS only ↴	Enable FTPS enforcement for enhanced security.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>
Function apps should use the latest TLS version ↴	Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the latest TLS version for Function apps to take advantage of security fixes, if any, and/or new functionalities of the latest version.	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↴</a>
Kubernetes clusters should be accessible only over HTTPS ↴	Use of HTTPS ensures authentication and protects data in transit from network layer eavesdropping attacks. This capability is currently generally available for Kubernetes Service (AKS), and in preview for Azure Arc enabled Kubernetes. For more info, visit <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> ↴	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">8.1.0 ↴</a>
Only secure connections to your Azure Cache for Redis should be enabled ↴	Audit enabling of only connections via SSL to Azure Cache for Redis. Use of secure connections ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking	Audit, Deny, Disabled	<a href="#">1.0.0 ↴</a>
Secure transfer to storage accounts should be enabled ↴	Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking	Audit, Deny, Disabled	<a href="#">2.0.0 ↴</a>
Windows machines should be configured to use secure	To protect the privacy of information communicated over the Internet, your machines should use the latest version of the industry-standard cryptographic protocol,	AuditIfNotExists, Disabled	<a href="#">4.1.1 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">communication protocols ↗</a>	Transport Layer Security (TLS). TLS secures communications over a network by encrypting a connection between machines.		

## Network Disconnect

ID: FedRAMP Moderate SC-10 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Reauthenticate or terminate a user session ↗</a>	CMA_0421 - Reauthenticate or terminate a user session	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Cryptographic Key Establishment And Management

ID: FedRAMP Moderate SC-12 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Preview]: Azure Recovery Services vaults should use customer-managed keys for encrypting backup data ↗</a>	Use customer-managed keys to manage the encryption at rest of your backup data. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/AB-CmkEncryption">https://aka.ms/AB-CmkEncryption</a> .	Audit, Deny, Disabled	<a href="#">1.0.0-preview ↗</a>
<a href="#">[Preview]: IoT Hub device provisioning service data should be encrypted using</a>	Use customer-managed keys to manage the encryption at rest of your IoT Hub device provisioning service. The data is automatically encrypted at rest with service-managed keys, but customer-managed keys (CMK) are commonly required to meet regulatory	Audit, Deny, Disabled	<a href="#">1.0.0-preview ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">customer-managed keys (CMK) ↗</a>	compliance standards. CMKs enable the data to be encrypted with an Azure Key Vault key created and owned by you. Learn more about CMK encryption at <a href="https://aka.ms/dps/CMK">https://aka.ms/dps/CMK</a> .		
<a href="#">Azure API for FHIR should use a customer-managed key to encrypt data at rest ↗</a>	Use a customer-managed key to control the encryption at rest of the data stored in Azure API for FHIR when this is a regulatory or compliance requirement. Customer-managed keys also deliver double encryption by adding a second layer of encryption on top of the default one done with service-managed keys.	audit, Audit, disabled, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Azure Automation accounts should use customer-managed keys to encrypt data at rest ↗</a>	Use customer-managed keys to manage the encryption at rest of your Azure Automation Accounts. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/automation-cmk">https://aka.ms/automation-cmk</a> .	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Batch account should use customer-managed keys to encrypt data ↗</a>	Use customer-managed keys to manage the encryption at rest of your Batch account's data. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/Batch-CMK">https://aka.ms/Batch-CMK</a> .	Audit, Deny, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Azure Container Instance container group should use customer-managed key for encryption ↗</a>	Secure your containers with greater flexibility using customer-managed keys. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Using customer-managed keys provides additional capabilities	Audit, Disabled, Deny	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	to control rotation of the key encryption key or cryptographically erase data.		
Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest <a href="#">↗</a>	<p>Use customer-managed keys to manage the encryption at rest of your Azure Cosmos DB. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards.</p> <p>Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/cosmosdb-cmk">https://aka.ms/cosmosdb-cmk</a> <a href="#">↗</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	1.1.0 <a href="#">↗</a>
Azure Data Box jobs should use a customer-managed key to encrypt the device unlock password <a href="#">↗</a>	Use a customer-managed key to control the encryption of the device unlock password for Azure Data Box. Customer-managed keys also help manage access to the device unlock password by the Data Box service in order to prepare the device and copy data in an automated manner. The data on the device itself is already encrypted at rest with Advanced Encryption Standard 256-bit encryption, and the device unlock password is encrypted by default with a Microsoft managed key.	Audit, Deny, Disabled	1.0.0 <a href="#">↗</a>
Azure Data Explorer encryption at rest should use a customer-managed key <a href="#">↗</a>	Enabling encryption at rest using a customer-managed key on your Azure Data Explorer cluster provides additional control over the key being used by the encryption at rest. This feature is oftentimes applicable to customers with special compliance requirements and requires a Key Vault to managing the keys.	Audit, Deny, Disabled	1.0.0 <a href="#">↗</a>
Azure data factories should be encrypted with a customer-managed key <a href="#">↗</a>	<p>Use customer-managed keys to manage the encryption at rest of your Azure Data Factory. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards.</p> <p>Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle,</p>	Audit, Deny, Disabled	1.0.1 <a href="#">↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	including rotation and management. Learn more at <a href="https://aka.ms/adf-cmk">https://aka.ms/adf-cmk</a> .		
<a href="#">Azure HDInsight clusters should use customer-managed keys to encrypt data at rest</a>	Use customer-managed keys to manage the encryption at rest of your Azure HDInsight clusters. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/hdi.cmk">https://aka.ms/hdi.cmk</a> .	Audit, Deny, Disabled	<a href="#">1.0.1</a>
<a href="#">Azure HDInsight clusters should use encryption at host to encrypt data at rest</a>	Enabling encryption at host helps protect and safeguard your data to meet your organizational security and compliance commitments. When you enable encryption at host, data stored on the VM host is encrypted at rest and flows encrypted to the Storage service.	Audit, Deny, Disabled	<a href="#">1.0.0</a>
<a href="#">Azure Machine Learning workspaces should be encrypted with a customer-managed key</a>	Manage encryption at rest of Azure Machine Learning workspace data with customer-managed keys. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/azureml-workspaces-cmk">https://aka.ms/azureml-workspaces-cmk</a> .	Audit, Deny, Disabled	<a href="#">1.0.3</a>
<a href="#">Azure Monitor Logs clusters should be encrypted with customer-managed key</a>	Create Azure Monitor logs cluster with customer-managed keys encryption. By default, the log data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance. Customer-managed key in Azure Monitor gives you more control over the access to your data, see	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">1.1.0</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<a href="https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys">https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys</a> .		
<a href="#">Azure Stream Analytics jobs should use customer-managed keys to encrypt data ↗</a>	Use customer-managed keys when you want to securely store any metadata and private data assets of your Stream Analytics jobs in your storage account. This gives you total control over how your Stream Analytics data is encrypted.	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Azure Synapse workspaces should use customer-managed keys to encrypt data at rest ↗</a>	Use customer-managed keys to control the encryption at rest of the data stored in Azure Synapse workspaces. Customer-managed keys deliver double encryption by adding a second layer of encryption on top of the default encryption with service-managed keys.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Bot Service should be encrypted with a customer-managed key ↗</a>	Azure Bot Service automatically encrypts your resource to protect your data and meet organizational security and compliance commitments. By default, Microsoft-managed encryption keys are used. For greater flexibility in managing keys or controlling access to your subscription, select customer-managed keys, also known as bring your own key (BYOK). Learn more about Azure Bot Service encryption: <a href="https://docs.microsoft.com/azure/bot-service/bot-service-encryption">https://docs.microsoft.com/azure/bot-service/bot-service-encryption</a> .	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Both operating systems and data disks in Azure Kubernetes Service clusters should be encrypted by customer-managed keys ↗</a>	Encrypting OS and data disks using customer-managed keys provides more control and greater flexibility in key management. This is a common requirement in many regulatory and industry compliance standards.	Audit, Deny, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Cognitive Services accounts should enable data encryption with</a>	Customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data stored in Cognitive Services to be encrypted with an Azure Key Vault key created and owned by you. You have full control and	Audit, Deny, Disabled	<a href="#">2.1.0 ↗</a>

<b>Name</b>  (Azure portal)	<b>Description</b>	<b>Effect(s)</b>	<b>Version</b>  (GitHub)
<a href="#">a customer-managed key</a>	responsibility for the key lifecycle, including rotation and management. Learn more about customer-managed keys at <a href="https://go.microsoft.com/fwlink/?linkid=2121321">https://go.microsoft.com/fwlink/?linkid=2121321</a> .		
<a href="#">Container registries should be encrypted with a customer-managed key</a>	Use customer-managed keys to manage the encryption at rest of the contents of your registries. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/acr/CMK">https://aka.ms/acr/CMK</a> .	Audit, Deny, Disabled	1.1.2
<a href="#">Define a physical key management process</a>	CMA_0115 - Define a physical key management process	Manual, Disabled	1.1.0
<a href="#">Define cryptographic use</a>	CMA_0120 - Define cryptographic use	Manual, Disabled	1.1.0
<a href="#">Define organizational requirements for cryptographic key management</a>	CMA_0123 - Define organizational requirements for cryptographic key management	Manual, Disabled	1.1.0
<a href="#">Determine assertion requirements</a>	CMA_0136 - Determine assertion requirements	Manual, Disabled	1.1.0
<a href="#">Event Hub namespaces should use a customer-managed key for encryption</a>	Azure Event Hubs supports the option of encrypting data at rest with either Microsoft-managed keys (default) or customer-managed keys. Choosing to encrypt data using customer-managed keys enables you to assign, rotate, disable, and revoke access to the keys that Event Hub will use to encrypt data in your namespace. Note that Event Hub only supports encryption with customer-	Audit, Disabled	1.0.0

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	managed keys for namespaces in dedicated clusters.		
<a href="#">HPC Cache accounts should use customer-managed key for encryption ↗</a>	Manage encryption at rest of Azure HPC Cache with customer-managed keys. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management.	Audit, Disabled, Deny	<a href="#">2.0.0 ↗</a>
<a href="#">Issue public key certificates ↗</a>	CMA_0347 - Issue public key certificates	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Logic Apps Integration Service Environment should be encrypted with customer-managed keys ↗</a>	Deploy into Integration Service Environment to manage encryption at rest of Logic Apps data using customer-managed keys. By default, customer data is encrypted with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Manage symmetric cryptographic keys ↗</a>	CMA_0367 - Manage symmetric cryptographic keys	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Managed disks should be double encrypted with both platform-managed and customer-managed keys ↗</a>	High security sensitive customers who are concerned of the risk associated with any particular encryption algorithm, implementation, or key being compromised can opt for additional layer of encryption using a different encryption algorithm/mode at the infrastructure layer using platform managed encryption keys. The disk encryption sets are required to use double encryption. Learn more at <a href="https://aka.ms/disks-doubleEncryption">https://aka.ms/disks-doubleEncryption</a> .	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">MySQL servers should use customer-managed keys to encrypt data at rest ↗</a>	<p>Use customer-managed keys to manage the encryption at rest of your MySQL servers. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards.</p> <p>Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management.</p>	AuditIfNotExists, Disabled	<a href="#">1.0.4 ↗</a>
<a href="#">OS and data disks should be encrypted with a customer-managed key ↗</a>	<p>Use customer-managed keys to manage the encryption at rest of the contents of your managed disks. By default, the data is encrypted at rest with platform-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards. Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more at <a href="https://aka.ms/disks-cmk">https://aka.ms/disks-cmk</a> ↗.</p>	Audit, Deny, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">PostgreSQL servers should use customer-managed keys to encrypt data at rest ↗</a>	<p>Use customer-managed keys to manage the encryption at rest of your PostgreSQL servers. By default, the data is encrypted at rest with service-managed keys, but customer-managed keys are commonly required to meet regulatory compliance standards.</p> <p>Customer-managed keys enable the data to be encrypted with an Azure Key Vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management.</p>	AuditIfNotExists, Disabled	<a href="#">1.0.4 ↗</a>
<a href="#">Restrict access to private keys ↗</a>	CMA_0445 - Restrict access to private keys	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Saved-queries in Azure Monitor should be saved in customer storage account</a>	Link storage account to Log Analytics workspace to protect saved-queries with storage account encryption. Customer-managed keys are commonly required to meet regulatory compliance and for more control over the access to your saved-queries	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">for logs encryption ↗</a>	in Azure Monitor. For more details on the above, see <a href="https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys?tabs=portal#customer-managed-key-for-saved-queries">https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys?tabs=portal#customer-managed-key-for-saved-queries</a> .		
<a href="#">Service Bus Premium namespaces should use a customer-managed key for encryption ↗</a>	Azure Service Bus supports the option of encrypting data at rest with either Microsoft-managed keys (default) or customer-managed keys. Choosing to encrypt data using customer-managed keys enables you to assign, rotate, disable, and revoke access to the keys that Service Bus will use to encrypt data in your namespace. Note that Service Bus only supports encryption with customer-managed keys for premium namespaces.	Audit, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">SQL managed instances should use customer-managed keys to encrypt data at rest ↗</a>	Implementing Transparent Data Encryption (TDE) with your own key provides you with increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties. This recommendation applies to organizations with a related compliance requirement.	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">SQL servers should use customer-managed keys to encrypt data at rest ↗</a>	Implementing Transparent Data Encryption (TDE) with your own key provides increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties. This recommendation applies to organizations with a related compliance requirement.	Audit, Deny, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Storage account encryption scopes should use customer-managed keys to encrypt data at rest ↗</a>	Use customer-managed keys to manage the encryption at rest of your storage account encryption scopes. Customer-managed keys enable the data to be encrypted with an Azure key-vault key created and owned by you. You have full control and responsibility for the key lifecycle, including rotation and management. Learn more about storage account encryption scopes at <a href="https://aka.ms/encryption-scopes-overview">https://aka.ms/encryption-scopes-overview</a> ↗.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Storage accounts should use customer-managed key for encryption ↗	Secure your blob and file storage account with greater flexibility using customer-managed keys. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Using customer-managed keys provides additional capabilities to control rotation of the key encryption key or cryptographically erase data.	Audit, Disabled	1.0.3 ↗

## Symmetric Keys

ID: FedRAMP Moderate SC-12 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Produce, control and distribute symmetric cryptographic keys ↗	CMA_C1645 - Produce, control and distribute symmetric cryptographic keys	Manual, Disabled	1.1.0 ↗

## Asymmetric Keys

ID: FedRAMP Moderate SC-12 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Produce, control and distribute asymmetric cryptographic keys ↗	CMA_C1646 - Produce, control and distribute asymmetric cryptographic keys	Manual, Disabled	1.1.0 ↗

## Cryptographic Protection

ID: FedRAMP Moderate SC-13 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define cryptographic use ↗</a>	CMA_0120 - Define cryptographic use	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Collaborative Computing Devices

ID: FedRAMP Moderate SC-15 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Explicitly notify use of collaborative computing devices ↗</a>	CMA_C1649 - Explicitly notify use of collaborative computing devices	Manual, Disabled	<a href="#">1.1.1 ↗</a>
<a href="#">Prohibit remote activation of collaborative computing devices ↗</a>	CMA_C1648 - Prohibit remote activation of collaborative computing devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Public Key Infrastructure Certificates

ID: FedRAMP Moderate SC-17 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Issue public key certificates ↗</a>	CMA_0347 - Issue public key certificates	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Mobile Code

ID: FedRAMP Moderate SC-18 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authorize, monitor, and control usage of mobile code</a>	CMA_C1653 - Authorize, monitor, and control usage of mobile code	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
technologies ↗	technologies		
Define acceptable and unacceptable mobile code technologies ↗	CMA_C1651 - Define acceptable and unacceptable mobile code technologies	Manual, Disabled	1.1.0 ↗
Establish usage restrictions for mobile code technologies ↗	CMA_C1652 - Establish usage restrictions for mobile code technologies	Manual, Disabled	1.1.0 ↗

## Voice Over Internet Protocol

ID: FedRAMP Moderate SC-19 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize, monitor, and control voip ↗	CMA_0025 - Authorize, monitor, and control voip	Manual, Disabled	1.1.0 ↗
Establish voip usage restrictions ↗	CMA_0280 - Establish voip usage restrictions	Manual, Disabled	1.1.0 ↗

## Secure Name / Address Resolution Service (Authoritative Source)

ID: FedRAMP Moderate SC-20 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement a fault tolerant name/address service ↗	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	1.1.0 ↗
Provide secure name and address resolution services ↗	CMA_0416 - Provide secure name and address resolution services	Manual, Disabled	1.1.0 ↗

# Secure Name /Address Resolution Service (Recursive Or Caching Resolver)

ID: FedRAMP Moderate SC-21 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement a fault tolerant name/address service ↗</a>	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Verify software, firmware and information integrity ↗</a>	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Architecture And Provisioning For Name/Address Resolution Service

ID: FedRAMP Moderate SC-22 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement a fault tolerant name/address service ↗</a>	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Session Authenticity

ID: FedRAMP Moderate SC-23 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Configure workstations to check for digital certificates ↗</a>	CMA_0073 - Configure workstations to check for digital certificates	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce random unique session identifiers ↗</a>	CMA_0247 - Enforce random unique session identifiers	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Protection Of Information At Rest

ID: FedRAMP Moderate SC-28 Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">App Service Environment should have internal encryption enabled ↗</a>	<p>Setting InternalEncryption to true encrypts the pagefile, worker disks, and internal network traffic between the front ends and workers in an App Service Environment. To learn more, refer to <a href="https://docs.microsoft.com/azure/app-service/environment/app-service-app-service-environment-custom-settings#enable-internal-encryption">https://docs.microsoft.com/azure/app-service/environment/app-service-app-service-environment-custom-settings#enable-internal-encryption</a>.</p>	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Automation account variables should be encrypted ↗</a>	<p>It is important to enable encryption of Automation account variable assets when storing sensitive data</p>	Audit, Deny, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Azure Data Box jobs should enable double encryption for data at rest on the device ↗</a>	<p>Enable a second layer of software-based encryption for data at rest on the device. The device is already protected via Advanced Encryption Standard 256-bit encryption for data at rest. This option adds a second layer of data encryption.</p>	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Monitor Logs clusters should be created with infrastructure-encryption enabled (double encryption) ↗</a>	<p>To ensure secure data encryption is enabled at the service level and the infrastructure level with two different encryption algorithms and two different keys, use an Azure Monitor dedicated cluster. This option is enabled by default when supported at the region, see <a href="https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys#customer-managed-key-overview">https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys#customer-managed-key-overview</a>.</p>	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Azure Stack Edge devices should use double-encryption ↗</a>	<p>To secure the data at rest on the device, ensure it's double-encrypted, the access to data is controlled, and once the device is deactivated, the data is securely erased off the data disks. Double encryption is the use of two layers of encryption: BitLocker XTS-AES 256-bit encryption on the data volumes and built-in encryption of the hard</p>	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	drives. Learn more in the security overview documentation for the specific Stack Edge device.		
Disk encryption should be enabled on Azure Data Explorer ↗	Enabling disk encryption helps protect and safeguard your data to meet your organizational security and compliance commitments.	Audit, Deny, Disabled	2.0.0 ↗
Double encryption should be enabled on Azure Data Explorer ↗	Enabling double encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. When double encryption has been enabled, data in the storage account is encrypted twice, once at the service level and once at the infrastructure level, using two different encryption algorithms and two different keys.	Audit, Deny, Disabled	2.0.0 ↗
Establish a data leakage management procedure ↗	CMA_0255 - Establish a data leakage management procedure	Manual, Disabled	1.1.0 ↗
Infrastructure encryption should be enabled for Azure Database for MySQL servers ↗	Enable infrastructure encryption for Azure Database for MySQL servers to have higher level of assurance that the data is secure. When infrastructure encryption is enabled, the data at rest is encrypted twice using FIPS 140-2 compliant Microsoft managed keys.	Audit, Deny, Disabled	1.0.0 ↗
Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers ↗	Enable infrastructure encryption for Azure Database for PostgreSQL servers to have higher level of assurance that the data is secure. When infrastructure encryption is enabled, the data at rest is encrypted twice using FIPS 140-2 compliant Microsoft managed keys	Audit, Deny, Disabled	1.0.0 ↗
Protect special information ↗	CMA_0409 - Protect special information	Manual, Disabled	1.1.0 ↗
Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign ↗	Service Fabric provides three levels of protection (None, Sign and EncryptAndSign) for node-to-node communication using a primary cluster certificate. Set the protection level to	Audit, Deny, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	ensure that all node-to-node messages are encrypted and digitally signed		
<a href="#">Storage accounts should have infrastructure encryption ↗</a>	Enable infrastructure encryption for higher level of assurance that the data is secure. When infrastructure encryption is enabled, data in a storage account is encrypted twice.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host ↗</a>	To enhance data security, the data stored on the virtual machine (VM) host of your Azure Kubernetes Service nodes VMs should be encrypted at rest. This is a common requirement in many regulatory and industry compliance standards.	Audit, Deny, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Transparent Data Encryption on SQL databases should be enabled ↗</a>	Transparent data encryption should be enabled to protect data-at-rest and meet compliance requirements	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Virtual machines and virtual machine scale sets should have encryption at host enabled ↗</a>	Use encryption at host to get end-to-end encryption for your virtual machine and virtual machine scale set data. Encryption at host enables encryption at rest for your temporary disk and OS/data disk caches. Temporary and ephemeral OS disks are encrypted with platform-managed keys when encryption at host is enabled. OS/data disk caches are encrypted at rest with either customer-managed or platform-managed key, depending on the encryption type selected on the disk. Learn more at <a href="https://aka.ms/vm-hbe">https://aka.ms/vm-hbe ↗</a> .	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources ↗</a>	By default, a virtual machine's OS and data disks are encrypted-at-rest using platform-managed keys. Temp disks, data caches and data flowing between compute and storage aren't encrypted. Disregard this recommendation if: 1. using encryption-at-host, or 2. server-side encryption on Managed Disks meets your security requirements. Learn more in: Server-side encryption of Azure Disk Storage: <a href="https://aka.ms/disksse">https://aka.ms/disksse, ↗</a> Different disk	AuditIfNotExists, Disabled	<a href="#">2.0.3 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
encryption offerings: <a href="https://aka.ms/diskencryptioncomparison">https://aka.ms/diskencryptioncomparison ↗</a>			

## Cryptographic Protection

ID: FedRAMP Moderate SC-28 (1) Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">App Service Environment should have internal encryption enabled ↗</a>	Setting InternalEncryption to true encrypts the pagefile, worker disks, and internal network traffic between the front ends and workers in an App Service Environment. To learn more, refer to <a href="https://docs.microsoft.com/azure/app-service/environment/app-service-app-service-environment-custom-settings#enable-internal-encryption">https://docs.microsoft.com/azure/app-service/environment/app-service-app-service-environment-custom-settings#enable-internal-encryption</a> .	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Automation account variables should be encrypted ↗</a>	It is important to enable encryption of Automation account variable assets when storing sensitive data	Audit, Deny, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Azure Data Box jobs should enable double encryption for data at rest on the device ↗</a>	Enable a second layer of software-based encryption for data at rest on the device. The device is already protected via Advanced Encryption Standard 256-bit encryption for data at rest. This option adds a second layer of data encryption.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Monitor Logs clusters should be created with infrastructure-encryption enabled (double encryption) ↗</a>	To ensure secure data encryption is enabled at the service level and the infrastructure level with two different encryption algorithms and two different keys, use an Azure Monitor dedicated cluster. This option is enabled by default when supported at the region, see <a href="https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys#customer-managed-key-overview">https://docs.microsoft.com/azure/azure-monitor/platform/customer-managed-keys#customer-managed-key-overview</a> .	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Azure Stack Edge devices should use</a>	To secure the data at rest on the device, ensure it's double-encrypted, the access to	audit, Audit, deny, Deny,	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">double-encryption ↗</a>	data is controlled, and once the device is deactivated, the data is securely erased off the data disks. Double encryption is the use of two layers of encryption: BitLocker XTS-AES 256-bit encryption on the data volumes and built-in encryption of the hard drives. Learn more in the security overview documentation for the specific Stack Edge device.	disabled, Disabled	
<a href="#">Disk encryption should be enabled on Azure Data Explorer ↗</a>	Enabling disk encryption helps protect and safeguard your data to meet your organizational security and compliance commitments.	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Double encryption should be enabled on Azure Data Explorer ↗</a>	Enabling double encryption helps protect and safeguard your data to meet your organizational security and compliance commitments. When double encryption has been enabled, data in the storage account is encrypted twice, once at the service level and once at the infrastructure level, using two different encryption algorithms and two different keys.	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Infrastructure encryption should be enabled for Azure Database for MySQL servers ↗</a>	Enable infrastructure encryption for Azure Database for MySQL servers to have higher level of assurance that the data is secure. When infrastructure encryption is enabled, the data at rest is encrypted twice using FIPS 140-2 compliant Microsoft managed keys.	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers ↗</a>	Enable infrastructure encryption for Azure Database for PostgreSQL servers to have higher level of assurance that the data is secure. When infrastructure encryption is enabled, the data at rest is encrypted twice using FIPS 140-2 compliant Microsoft managed keys	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Protect data in transit using encryption ↗</a>	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s) (GitHub)	Version
<a href="#">Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign ↴</a>	Service Fabric provides three levels of protection (None, Sign and EncryptAndSign) for node-to-node communication using a primary cluster certificate. Set the protection level to ensure that all node-to-node messages are encrypted and digitally signed	Audit, Deny, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Storage accounts should have infrastructure encryption ↴</a>	Enable infrastructure encryption for higher level of assurance that the data is secure. When infrastructure encryption is enabled, data in a storage account is encrypted twice.	Audit, Deny, Disabled	<a href="#">1.0.0 ↴</a>
<a href="#">Temp disks and cache for agent node pools in Azure Kubernetes Service clusters should be encrypted at host ↴</a>	To enhance data security, the data stored on the virtual machine (VM) host of your Azure Kubernetes Service nodes VMs should be encrypted at rest. This is a common requirement in many regulatory and industry compliance standards.	Audit, Deny, Disabled	<a href="#">1.0.1 ↴</a>
<a href="#">Transparent Data Encryption on SQL databases should be enabled ↴</a>	Transparent data encryption should be enabled to protect data-at-rest and meet compliance requirements	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↴</a>
<a href="#">Virtual machines and virtual machine scale sets should have encryption at host enabled ↴</a>	Use encryption at host to get end-to-end encryption for your virtual machine and virtual machine scale set data. Encryption at host enables encryption at rest for your temporary disk and OS/data disk caches. Temporary and ephemeral OS disks are encrypted with platform-managed keys when encryption at host is enabled. OS/data disk caches are encrypted at rest with either customer-managed or platform-managed key, depending on the encryption type selected on the disk. Learn more at <a href="https://aka.ms/vm-hbe">https://aka.ms/vm-hbe</a> ↴.	Audit, Deny, Disabled	<a href="#">1.0.0 ↴</a>
<a href="#">Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources ↴</a>	By default, a virtual machine's OS and data disks are encrypted-at-rest using platform-managed keys. Temp disks, data caches and data flowing between compute and storage aren't encrypted. Disregard this recommendation if: 1. using encryption-at-host, or 2. server-side encryption on	AuditIfNotExists, Disabled	<a href="#">2.0.3 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>Managed Disks meets your security requirements. Learn more in: Server-side encryption of Azure Disk Storage:  <a href="https://aka.ms/disksse">https://aka.ms/disksse</a>, ↗ Different disk encryption offerings:  <a href="https://aka.ms/diskencryptioncomparison">https://aka.ms/diskencryptioncomparison</a> ↗</p>		

## Process Isolation

ID: FedRAMP Moderate SC-39 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Maintain separate execution domains for running processes</a> ↗	CMA_C1665 - Maintain separate execution domains for running processes	Manual, Disabled	<a href="#">1.1.0</a> ↗

## System And Information Integrity

### System And Information Integrity Policy And Procedures

ID: FedRAMP Moderate SI-1 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update information integrity policies and procedures</a> ↗	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	<a href="#">1.1.0</a> ↗

## Flaw Remediation

ID: FedRAMP Moderate SI-2 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s) (GitHub)	Version
<a href="#">A vulnerability assessment solution should be enabled on your virtual machines ↗</a>	Audits virtual machines to detect whether they are running a supported vulnerability assessment solution. A core component of every cyber risk and security program is the identification and analysis of vulnerabilities. Azure Security Center's standard pricing tier includes vulnerability scanning for your virtual machines at no extra cost. Additionally, Security Center can automatically deploy this tool for you.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">App Service apps should use latest 'HTTP Version' ↗</a>	Periodically, newer versions are released for HTTP either due to security flaws or to include additional functionality. Using the latest HTTP version for web apps to take advantage of security fixes, if any, and/or new functionalities of the newer version.	AuditIfNotExists, Disabled	<a href="#">4.0.0 ↗</a>
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	potentially harmful attempts to access or exploit key vault accounts.		
Azure Defender for Resource Manager should be enabled ↴	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	1.0.0 ↴
Azure Defender for servers should be enabled ↴	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↴
Azure Defender for SQL servers on machines should be enabled ↴	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↴
Function apps should use latest 'HTTP Version' ↴	Periodically, newer versions are released for HTTP either due to security flaws or to include additional functionality. Using the latest HTTP version for web apps to take advantage of security fixes, if any, and/or new functionalities of the newer version.	AuditIfNotExists, Disabled	4.0.0 ↴
Incorporate flaw remediation into configuration management ↴	CMA_C1671 - Incorporate flaw remediation into configuration management	Manual, Disabled	1.1.0 ↴
Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version ↴	Upgrade your Kubernetes service cluster to a later Kubernetes version to protect against known vulnerabilities in your current Kubernetes version. Vulnerability CVE-2019-9946 has been patched in Kubernetes versions 1.11.9+, 1.12.7+, 1.13.5+, and 1.14.0+	Audit, Disabled	1.0.2 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Microsoft Defender for Containers should be enabled ↗</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">SQL databases should have vulnerability findings resolved ↗</a>	Monitor vulnerability assessment scan results and recommendations for how to remediate database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">4.1.0 ↗</a>
<a href="#">System updates on virtual machine scale sets should be installed ↗</a>	Audit whether there are any missing system security updates and critical updates that should be installed to ensure that your Windows and Linux virtual machine scale sets are secure.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">System updates should be installed on your machines ↗</a>	Missing security system updates on your servers will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">4.0.0 ↗</a>
<a href="#">Vulnerabilities in security configuration on your machines should be remediated ↗</a>	Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
<a href="#">Vulnerabilities in security configuration on your virtual machine scale sets</a>	Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">should be remediated ↗</a>			

## Automated Flaw Remediation Status

ID: FedRAMP Moderate SI-2 (2) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">Automate flaw remediation ↗</a>	CMA_0027 - Automate flaw remediation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Time To Remediate Flaws / Benchmarks For Corrective Actions

ID: FedRAMP Moderate SI-2 (3) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">Establish benchmarks for flaw remediation ↗</a>	CMA_C1675 - Establish benchmarks for flaw remediation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Measure the time between flaw identification and flaw remediation ↗</a>	CMA_C1674 - Measure the time between flaw identification and flaw remediation	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Malicious Code Protection

ID: FedRAMP Moderate SI-3 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↗
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↗
Endpoint protection solution should be installed on virtual machine scale sets ↗	Audit the existence and health of an endpoint protection solution on your virtual machines scale sets, to protect them from threats and vulnerabilities.	AuditIfNotExists, Disabled	3.0.0 ↗
Manage gateways ↗ CMA_0363 - Manage gateways		Manual, Disabled	1.1.0 ↗
Monitor missing Endpoint Protection in Azure Security Center ↗	Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.0.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Review malware detections report weekly ↗	CMA_0475 - Review malware detections report weekly	Manual, Disabled	1.1.0 ↗
Review threat protection status weekly ↗	CMA_0479 - Review threat protection status weekly	Manual, Disabled	1.1.0 ↗
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗
Windows Defender Exploit Guard should be enabled on your machines ↗	Windows Defender Exploit Guard uses the Azure Policy Guest Configuration agent. Exploit Guard has four components that are designed to lock down devices against a wide variety of attack vectors and block behaviors	AuditIfNotExists, Disabled	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	commonly used in malware attacks while enabling enterprises to balance their security risk and productivity requirements (Windows only).		

## Central Management

ID: FedRAMP Moderate SI-3 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Azure Defender for servers should be enabled ↴</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>
<a href="#">Block untrusted and unsigned processes that run from USB ↴</a>	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Endpoint protection solution should be installed on virtual machine scale sets ↴</a>	Audit the existence and health of an endpoint protection solution on your virtual machines scale sets, to protect them from threats and vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>
<a href="#">Manage gateways ↴</a>	CMA_0363 - Manage gateways	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Monitor missing Endpoint Protection in Azure Security Center ↴</a>	Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>
<a href="#">Perform a trend analysis on threats ↴</a>	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Perform vulnerability scans ↴</a>	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review malware detections report weekly ↗	CMA_0475 - Review malware detections report weekly	Manual, Disabled	1.1.0 ↗
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗
Windows Defender Exploit Guard should be enabled on your machines ↗	Windows Defender Exploit Guard uses the Azure Policy Guest Configuration agent. Exploit Guard has four components that are designed to lock down devices against a wide variety of attack vectors and block behaviors commonly used in malware attacks while enabling enterprises to balance their security risk and productivity requirements (Windows only).	AuditIfNotExists, Disabled	2.0.0 ↗

## Automatic Updates

ID: FedRAMP Moderate SI-3 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↗
Manage gateways ↗	CMA_0363 - Manage gateways	Manual, Disabled	1.1.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Review malware detections report weekly ↗	CMA_0475 - Review malware detections report weekly	Manual, Disabled	1.1.0 ↗
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗

## Nonsignature-Based Detection

ID: FedRAMP Moderate SI-3 (7) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↗
Manage gateways ↗	CMA_0363 - Manage gateways	Manual, Disabled	1.1.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Review malware detections report weekly ↗	CMA_0475 - Review malware detections report weekly	Manual, Disabled	1.1.0 ↗
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗

## Information System Monitoring

ID: FedRAMP Moderate SI-4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: All Internet traffic should be routed via your deployed Azure Firewall ↗	Azure Security Center has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall	AuditIfNotExists, Disabled	3.0.0-preview ↗
[Preview]: Azure Arc enabled Kubernetes	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and	AuditIfNotExists, Disabled	6.0.0-preview ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">clusters should have Microsoft Defender for Cloud extension installed ↗</a>	sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivot=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivot=defender-for-container-arc</a> .		
<a href="#">[Preview]: Log Analytics extension should be installed on your Linux Azure Arc machines ↗</a>	This policy audits Linux Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	<a href="#">1.0.1-preview ↗</a>
<a href="#">[Preview]: Log Analytics extension should be installed on your Windows Azure Arc machines ↗</a>	This policy audits Windows Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	<a href="#">1.0.1-preview ↗</a>
<a href="#">[Preview]: Network traffic data collection agent should be installed on Linux virtual machines ↗</a>	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	<a href="#">1.0.2-preview ↗</a>
<a href="#">[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗</a>	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	<a href="#">1.0.2-preview ↗</a>
<a href="#">Auto provisioning of the Log Analytics agent should be enabled on</a>	To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">your subscription ↗</a>	and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.		
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Resource Manager should be enabled ↗</a>	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for servers should be enabled ↴	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>
Azure Defender for SQL servers on machines should be enabled ↴	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↴	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↴</a>
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↴	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>
Guest Configuration extension should be installed on your machines ↴	To ensure secure configurations of in-guest settings of your machine, install the Guest Configuration extension. In-guest settings that the extension monitors include the configuration of the operating system, application configuration or presence, and environment settings. Once installed, in-guest policies will be available such as 'Windows Exploit guard should be enabled'. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>
Log Analytics agent should be installed on your virtual machine for Azure Security	This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Center monitoring ↗</a>			
<a href="#">Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring ↗</a>	Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Containers should be enabled ↗</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Network Watcher should be enabled ↗</a>	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Obtain legal opinion for monitoring system activities ↗</a>	CMA_C1688 - Obtain legal opinion for monitoring system activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform a trend analysis on threats ↴	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↴
Provide monitoring information as needed ↴	CMA_C1689 - Provide monitoring information as needed	Manual, Disabled	1.1.0 ↴
Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity ↴	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴	AuditIfNotExists, Disabled	1.0.1 ↴

## Automated Tools For Real-Time Analysis

ID: FedRAMP Moderate SI-4 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security operations ↴	CMA_0202 - Document security operations	Manual, Disabled	1.1.0 ↴
Turn on sensors for endpoint security solution ↴	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	1.1.0 ↴

## Inbound And Outbound Communications Traffic

ID: FedRAMP Moderate SI-4 (4) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize, monitor, and control voip ↗	CMA_0025 - Authorize, monitor, and control voip	Manual, Disabled	1.1.0 ↗
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	1.1.0 ↗
Manage gateways ↗	CMA_0363 - Manage gateways	Manual, Disabled	1.1.0 ↗
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	1.1.0 ↗

## System-Generated Alerts

ID: FedRAMP Moderate SI-4 (5) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Alert personnel of information spillage ↗	CMA_0007 - Alert personnel of information spillage	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Set automated notifications for new and trending cloud applications in your organization ↗	CMA_0495 - Set automated notifications for new and trending cloud applications in your organization	Manual, Disabled	1.1.0 ↗

## Wireless Intrusion Detection

ID: FedRAMP Moderate SI-4 (14) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document wireless access security controls ↗	CMA_C1695 - Document wireless access security controls	Manual, Disabled	1.1.0 ↗

# Security Alerts, Advisories, And Directives

ID: FedRAMP Moderate SI-5 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Disseminate security alerts to personnel ↗	CMA_C1705 - Disseminate security alerts to personnel	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a threat intelligence program ↗	CMA_0260 - Establish a threat intelligence program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Generate internal security alerts ↗	CMA_C1704 - Generate internal security alerts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement security directives ↗	CMA_C1706 - Implement security directives	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Security Function Verification

ID: FedRAMP Moderate SI-6 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Create alternative actions for identified anomalies ↗	CMA_C1711 - Create alternative actions for identified anomalies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify personnel of any failed security verification tests ↗	CMA_C1710 - Notify personnel of any failed security verification tests	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform security function verification at a defined frequency ↗	CMA_C1709 - Perform security function verification at a defined frequency	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify security functions ↗	CMA_C1708 - Verify security functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Software, Firmware, And Information Integrity

ID: FedRAMP Moderate SI-7 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Verify software, firmware and information integrity ↗</a>	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Integrity Checks

ID: FedRAMP Moderate SI-7 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Verify software, firmware and information integrity ↗</a>	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">View and configure system diagnostic data ↗</a>	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information Input Validation

ID: FedRAMP Moderate SI-10 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Perform information input validation ↗</a>	CMA_C1723 - Perform information input validation	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Error Handling

ID: FedRAMP Moderate SI-11 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Generate error messages ↗</a>	CMA_C1724 - Generate error messages	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Reveal error messages ↗</a>	CMA_C1725 - Reveal error messages	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information Handling And Retention

ID: FedRAMP Moderate SI-12 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage the input, output, processing, and storage of data ↗</a>	CMA_0369 - Manage the input, output, processing, and storage of data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review label activity and analytics ↗</a>	CMA_0474 - Review label activity and analytics	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Memory Protection

ID: FedRAMP Moderate SI-16 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Azure Defender for servers should be enabled ↗</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Windows Defender Exploit Guard should be enabled on your machines ↗</a>	Windows Defender Exploit Guard uses the Azure Policy Guest Configuration agent. Exploit Guard has four components that are designed to lock down devices against a wide variety of attack vectors and block behaviors commonly	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Used in malware attacks while enabling enterprises to balance their security risk and productivity requirements (Windows only).		

## Next steps

Additional articles about Azure Policy:

- [Regulatory Compliance](#) overview.
- See the [initiative definition structure](#).
- Review other examples at [Azure Policy samples](#).
- Review [Understanding policy effects](#).
- Learn how to [remediate non-compliant resources](#).

# FedRAMP compliance program overview

Article • 05/31/2023

Accelerating your path to the US Federal Risk and Authorization Management Program (FedRAMP) compliance in Azure is a focused effort that provides learning resources and implementation tools. The goal is education and support during the scoping and implementation of your project. Moreover, Microsoft works with key assessment and automation partners to share reference architectures and solutions that can help you meet your compliance needs.

As a partner who provides a service in this field, you can publish your offering in the marketplace that expands the reach of your service.

## Customers

US Government agencies and many other organizations rely on commercial software companies to achieve their missions. FedRAMP was established to provide a standardized approach for assessing, monitoring, and authorizing cloud computing products and services. This approach uses a "do once, use many times" framework that saves cost, time, and resources required to conduct individual agency security assessments. FedRAMP is based on the National Institute of Standards and Technology (NIST) SP 800-53 standard, augmented by FedRAMP controls and control enhancements.

There are two types of FedRAMP authorizations for cloud services:

- A Provisional Authority to Operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB)
- An agency Authority to Operate (ATO)

## P-ATO process

A FedRAMP P-ATO is an initial approval of the cloud service provider (CSP) authorization package by the JAB. An agency can rely on P-ATO to grant an ATO for the acquisition and use of the cloud service within their agency. The JAB consists of the Chief Information Officers (CIOs) from the US Department of Defense (DoD), Department of Homeland Security (DHS), and General Services Administration (GSA), supported by designated technical representatives (TRs) from their respective member organizations.

A P-ATO means that the JAB has reviewed the cloud service's authorization package and provided a provisional approval for federal agencies to use when granting an ATO for a cloud services offering.

## Agency ATO process

As part of the agency authorization process, a CSP works directly with the agency sponsor who reviews the cloud service's security package. After completing a security assessment, the head of an agency (or their designee) can grant an ATO.

Consequently, an ISV can choose to go for a JAB authorization, which grants a generalized authorization to its solution and can be used with multiple agencies. This process tends to be longer. They can also choose to go for an agency ATO, which is specific to the Government customer they're serving. This customer acts as the sponsor and may even have "reciprocity" with other agencies, which allows for a faster, smoother adoption of the company's solution with a different customer.

## Partners

Microsoft is able to scale through its partners. Scale is what allows us to create a more predictable, cost-effective, and speedy delivery. These concerns are also common with pursuing an ATO. We're focused on enabling two main kinds of partnerships:

- **Advisory:** enables partners to create offerings based on Azure that guide a customer through individual steps or the entire ATO process. These partners offer consulting services bundled with some automated solutions that add value to Azure Marketplace compliance offerings. They can usually be contracted directly, by reference, or via Microsoft Azure Marketplace.
- **Automation:** there are two types of automation partners we focus on:
  - Foundational partners, which enable integration of third party solutions with Azure and help you achieve / meet controls from your FedRAMP package. These partners are part of our recommended reference architectures.
  - True automation partners that help automate certain aspects of the ATO journey such as the FedRAMP System Security Plan (SSP) generation, self-healing, alerts, and monitoring.

### ⓘ Note

Partners are asked to publish their solutions to Azure Marketplace. See the following steps for guidance.

# Publishing to Azure Marketplace

1. Join the Partner Network – It's a requirement for publishing but easy to sign up.  
For instructions, see [Create a Partner Center account and enroll in the commercial marketplace](#).
2. Enable your partner center account as Publisher / Developer for Marketplace by following the instructions in [Create a commercial marketplace account in Partner Center](#).
3. With an enabled Partner Center Account, publish your listing as a SaaS application as explained in [Create a SaaS offer](#).

For a list of existing Azure Marketplace offerings in this space, visit [Azure Marketplace](#).

## More resources

### Note

The information provided here will allow you to sign up and learn about the FedRAMP compliance program. The program is designed to help Azure and Azure Government customers successfully prepare their environments for authorization and request a FedRAMP ATO. This information does not constitute an offer of any kind, and submitting the following forms in no way guarantees participation in the program. Currently, the program details shared with partners and customers are notional and subject to change without notice.

- [FedRAMP training resources](#).
- [FedRAMP documents and templates](#) to help you with program requirements.
- Get familiar with the [FedRAMP Marketplace](#).
- Learn more about [Azure Government compliance](#).

## Next steps

Review the [Publishing guide by offer type](#) for further tips and troubleshooting. If you're still facing issues, open a ticket in Partner Center.

# Internal Revenue Service (IRS) Publication 1075

Article • 04/06/2023

## IRS 1075 overview

Internal Revenue Service [Publication 1075](#) (IRS 1075) provides safeguards for protecting Federal Tax Information (FTI) at all points where it is received, processed, stored, and maintained. It applies to federal, state, and local agencies with whom IRS shares FTI, and it defines a broad set of management, operations, and technology specific security controls that must be in place to protect FTI. Additional requirements cover the protection of FTI in a cloud computing environment (also known as [Exhibit 16](#)), and place much emphasis on FIPS 140 validated [data encryption](#) in transit and at rest.

To protect FTI, IRS 1075 prescribes security and privacy controls for application, platform, and datacenter services. For instance, it prioritizes the security of datacenter activities, such as the proper handling of FTI, and the oversight of datacenter contractors to limit entry. To ensure that government agencies receiving FTI apply those controls, the IRS established the Safeguards Program, which includes periodic reviews of these agencies and their contractors. For more information, see *Mandatory Requirements for FTI in a Cloud Environment* available from the Safeguards Program [Cloud Computing Environment](#) page.

## Azure and IRS 1075

The US [Federal Risk and Authorization Management Program](#) (FedRAMP) was established to provide a standardized approach for assessing, monitoring, and authorizing cloud computing products and services. FedRAMP is based on the National Institute of Standards and Technology (NIST) [SP 800-53](#) standard, augmented by FedRAMP controls and control enhancements. Microsoft maintains a [FedRAMP High Provisional Authorization to Operate \(P-ATO\)](#) issued by the FedRAMP Joint Authorization Board (JAB) for both Azure and Azure Government cloud environments. The IRS 1075 core control scope is based on NIST SP 800-53 control requirements that Azure services cover as part of the existing FedRAMP High P-ATOs. Azure services provide extensive controls for data encryption in transit and at rest to support IRS 1075 requirements for the protection of FTI in a cloud computing environment. These controls enable you to encrypt FTI using [FIPS 140](#) validated cryptography and rely on

Azure Key Vault to store your encryption keys in FIPS 140 validated hardware security modules (HSMs) under your control, also known as customer-managed keys (CMK).

For extra customer assistance, Microsoft provides the Azure Policy regulatory compliance built-in initiatives for Azure and Azure Government, which map to IRS 1075 compliance domains and controls:

- [IRS 1075 Azure regulatory compliance built-in initiative](#)
- [IRS 1075 Azure Government regulatory compliance built-in initiative](#)

Regulatory compliance in Azure Policy provides built-in initiative definitions to view a list of controls and compliance domains based on responsibility – customer, Microsoft, or shared. For Microsoft-responsible controls, we provide extra audit result details based on third-party attestations and our control implementation details to achieve that compliance. Each IRS 1075 control is associated with one or more Azure Policy definitions. These policies may help you [assess compliance](#) with the control; however, compliance in Azure Policy is only a partial view of your overall compliance status. Azure Policy helps to enforce organizational standards and assess compliance at scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to more granular status.

Microsoft also provides contractual amendments for both Azure and Azure Government to demonstrate that these cloud environments have appropriate security controls and capabilities in place necessary for you to meet the substantive IRS 1075 requirements. Contact your Microsoft account team to obtain these documents.

## FTI encryption

Azure enables you to encrypt your data [in transit](#) and [at rest](#) to support IRS 1075 requirements for the protection of FTI in a cloud computing environment, including FIPS 140 validated data encryption. FTI encryption requirements are part of the *Mandatory Requirements for FTI in a Cloud Environment* that are described on the Safeguards Program [Cloud Computing Environment](#) page. As stated, "Agencies must retain control of the encryption keys used to encrypt and decrypt the FTI at all times and be able to provide information as to who has access to and knows information regarding the key passphrase. If the agency is able to satisfy this requirement, effectively preventing logical access to the data from the cloud vendor, agencies may use cloud infrastructure for data types that have contractor-access restrictions."

You can implement extra security for your sensitive data, such as FTI, stored in Azure services by encrypting it using your own encryption keys you control in [Azure Key Vault](#), which is an Azure service for securely storing and managing secrets, including your

cryptographic keys. You can use [FIPS 140](#) validated cryptography and rely on Azure Key Vault to store your encryption keys in FIPS 140 validated hardware security modules (HSMs) under your control, also known as customer-managed keys (CMK).

Azure Key Vault offers [strong assurances](#) about customer sole control over encryption keys and corresponding data access:

- Azure Key Vault and Azure Key Vault Managed HSM are designed, deployed and operated such that Microsoft and its agents are precluded from accessing, using or extracting any data stored in the service, including cryptographic keys.
- With Key Vault, you can import or generate encryption keys in HSMs, ensuring that keys never leave the HSM protection boundary to support *bring your own key (BYOK)* scenarios.
- Keys generated inside the Key Vault HSMs aren't exportable – there can be no clear-text version of the key outside the HSMs. This binding is enforced by the underlying HSM.
- FIPS 140 validation of Key Vault HSMs includes evidence of physical tamper resistance.
- The Key Vault team explicitly doesn't have operating procedures for granting such access to Microsoft and its agents, even if authorized by a customer.

Therefore, if you use CMK stored in Azure Key Vault HSMs, you effectively maintain sole ownership of encryption keys, as recommended by the IRS Office of Safeguards. For more information, see [Data encryption key management](#).

## Applicability

- Azure
- Azure Government

## Office 365 and IRS 1075

For more information about Office 365 compliance, see [Office 365 IRS 1075 documentation](#).

## Guidance documents

For instructions on how to access guidance documents, see [Audit documentation](#). The following documents are available from the Service Trust Portal (STP) [United States Government](#) section:

- Azure Commercial – IRS Safeguards 45-day Cloud Computing Notification Form
- Azure Government – IRS Safeguards 45-day Cloud Computing Notification Form

These documents are pre-filled with Microsoft responses to help you submit a 45-day notification form to the IRS Office of Safeguards, as explained on the Safeguards Program [cloud computing environment](#) page.

If you're subject to IRS 1075 compliance requirements, you can contact your Microsoft account representative to request the following documents:

- Microsoft IRS 1075 contractual amendment for Azure
- Microsoft IRS 1075 contractual amendment for Azure Government

These contractual amendments demonstrate that Azure and Azure Government have appropriate security controls and capabilities in place necessary for you to meet the substantive IRS 1075 requirements.

## Frequently asked questions

### How do Azure and Azure Government address the requirements of IRS 1075?

Both Azure and Azure Government maintains a [FedRAMP High P-ATO](#) issued by the JAB. The IRS 1075 core control scope is based on NIST SP 800-53 control requirements that Azure and Azure Government cover as part of the existing FedRAMP High P-ATO. Azure services enable you to encrypt FTI in transit and at rest using FIPS 140 validated cryptography, and maintain sole control over encryption keys in FIPS 140 validated hardware security modules (HSMs), also known as customer-managed keys (CMK). For extra customer assistance, Microsoft provides the Azure Policy regulatory compliance built-in initiatives for both [Azure](#) and [Azure Government](#), which maps to IRS 1075 compliance domains and controls. Finally, Microsoft can provide you with contractual amendments to demonstrate that Azure and Azure Government have appropriate security controls and capabilities in place necessary for you to meet the substantive IRS 1075 requirements.

### Can I review the FedRAMP packages or the System Security Plan?

Yes. You can request Azure and Azure Government FedRAMP documentation directly from the [FedRAMP Marketplace](#) by submitting a package access request form. You must have a .gov or .mil email address to access a FedRAMP security package directly from FedRAMP. Azure Commercial FedRAMP System Security Plan is available to customers under NDA from the Service Trust Portal [FedRAMP reports](#) section. For instructions on how to access audit reports and certificates, see [Audit documentation](#). Select Azure Government FedRAMP documentation, including the System Security Plan (SSP), continuous monitoring reports, Plan of Action and Milestones (POA&M), and so

on, are available under NDA and pending access authorization from the Service Trust Portal [FedRAMP reports](#) section. Contact your Microsoft account representative for assistance.

### Can Azure accommodate 5.6 *Human Services Agencies—IRC 6103(l)(7)* requirements stated in IRS 1075?

Yes. See Section 5 in the FTI 45-day Cloud Notification Form where IRC 6103(l)(7) requirements are clarified, and then review Microsoft responses as explained in [Guidance documents](#). IRC 6103(l)(7) stipulates, among other things, that "Human services agencies may not contract for services that involve the disclosure of FTI to contractors". FTI Cloud Notification Form clarifies that "If the agency is able to encrypt data using FIPS 140 certified solutions and maintain sole ownership of encryption keys, Safeguards will consider this a logical barrier and will allow data types with restrictions (e.g., (l)(7)) to move to a cloud environment." You can [encrypt your data](#) stored in Azure services using [FIPS 140](#) validated cryptography and use Azure Key Vault to [store your encryption keys](#) in FIPS 140 validated hardware security modules (HSMs) under your control, also known as customer-managed keys (CMK).

### Should I use Azure or Azure Government for workloads that are subject to IRS Publication 1075 requirements?

If you are subject to IRS 1075 compliance obligations, both Azure and Azure Government can help you meet those obligations. The decision will rest with you based on your business requirements. Both Azure and Azure Government have the same security controls in place, including the same provisions for the safeguarding of FTI in transit and at rest. Most state and local government agencies are best aligned with Azure Government, which provides an extra layer of protection to customers through contractual commitments regarding storage of customer data in the United States and limiting potential access to systems processing customer data to [screened US persons](#). However, the need to meet your IRS 1075 compliance requirements isn't a deciding factor for choosing your cloud environment.

## Resources

- [Azure compliance documentation](#)
- [Azure enables a world of compliance](#)
- [Microsoft 365 compliance offerings](#)
- [Compliance on the Microsoft Trust Center](#)
- [What is Azure Government?](#)
- [Explore Azure Government](#)
- [Microsoft government solutions](#)
- Internal Revenue Service [Publication 1075](#) (IRS 1075)

- [IRS Safeguards Program](#)
- [Mandatory requirements for FTI in a cloud environment](#) as shown on the Safeguards Program cloud computing environment page
- [Exhibit 16](#) *IRS Office of Safeguards Technical Assistance Memorandum: Protecting Federal Tax Information (FTI) In a Cloud Computing Environment*
- [Encryption Requirements of Publication 1075](#)
- [NIST SP 800-53](#) *Security and Privacy Controls for Information Systems and Organizations*

# Details of the IRS 1075 September 2016 (Azure Government) Regulatory Compliance built-in initiative

Article • 01/02/2024

The following article details how the Azure Policy Regulatory Compliance built-in initiative definition maps to **compliance domains** and **controls** in IRS 1075 September 2016 (Azure Government). For more information about this compliance standard, see [IRS 1075 September 2016](#). To understand *Ownership*, see [Azure Policy policy definition](#) and [Shared responsibility in the cloud](#).

The following mappings are to the [IRS 1075 September 2016](#) controls. Many of the controls are implemented with an [Azure Policy](#) initiative definition. To review the complete initiative definition, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the [IRS1075 September 2016](#) Regulatory Compliance built-in initiative definition.

## Important

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policy definitions themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between compliance domains, controls, and Azure Policy definitions for this compliance standard may change over time. To view the change history, see the [GitHub Commit History](#).

## Access Control

### Remote Access (AC-17)

ID: IRS 1075 9.3.1.12

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	1.2.0 ↗
Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	1.2.0 ↗
App Service apps should have remote debugging turned off ↗	Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0 ↗
Audit Linux machines that allow remote connections from accounts without passwords ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Linux machines that allow remote connections from accounts without passwords	AuditIfNotExists, Disabled	1.3.0 ↗
Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↗	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	1.3.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Function apps should have remote debugging turned off ↴	Remote debugging requires inbound ports to be opened on Function apps. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0 ↴
Storage accounts should restrict network access ↴	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges	Audit, Deny, Disabled	1.1.1 ↴

## Account Management (AC-2)

ID: IRS 1075 9.3.1.2

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An Azure Active Directory administrator should be provisioned for SQL servers ↴	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	1.0.0 ↴
Audit usage of custom RBAC roles ↴	Audit built-in roles such as 'Owner', 'Contributer', 'Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling	Audit, Disabled	1.0.1 ↴
Blocked accounts with owner permissions on Azure resources should be removed ↴	Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in.	AuditIfNotExists, Disabled	1.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Blocked accounts with read and write permissions on Azure resources should be removed ↴	Deprecated accounts should be removed from your subscriptions. Deprecated accounts are accounts that have been blocked from signing in.	AuditIfNotExists, Disabled	1.0.0 ↴
Guest accounts with owner permissions on Azure resources should be removed ↴	External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.	AuditIfNotExists, Disabled	1.0.0 ↴
Guest accounts with read permissions on Azure resources should be removed ↴	External accounts with read privileges should be removed from your subscription in order to prevent unmonitored access.	AuditIfNotExists, Disabled	1.0.0 ↴
Guest accounts with write permissions on Azure resources should be removed ↴	External accounts with write privileges should be removed from your subscription in order to prevent unmonitored access.	AuditIfNotExists, Disabled	1.0.0 ↴
Management ports of virtual machines should be protected with just-in-time network access control ↴	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.0.0 ↴
Service Fabric clusters should only use Azure Active Directory for client authentication ↴	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	1.1.0 ↴

## Information Flow Enforcement (AC-4)

ID: IRS 1075 9.3.1.4

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
App Service apps should not have CORS configured to allow every resource to access your apps ↴	Cross-Origin Resource Sharing (CORS) should not allow all domains to access your app. Allow only	AuditIfNotExists, Disabled	2.0.0 ↴

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
	required domains to interact with your app.		

## Separation of Duties (AC-5)

ID: IRS 1075 9.3.1.5

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">A maximum of 3 owners should be designated for your subscription ↗</a>	It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	modify	<a href="#">1.2.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	modify	<a href="#">1.2.0 ↗</a>
<a href="#">Audit Windows machines missing any of specified members in the</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if the local Administrators group	auditIfNotExists	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Administrators group ↗</a>	does not contain one or more members that are listed in the policy parameter.		
<a href="#">Audit Windows machines that have the specified members in the Administrators group ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if the local Administrators group contains one or more of the members listed in the policy parameter.	auditIfNotExists	<a href="#">1.0.0 ↗</a>
<a href="#">Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs ↗</a>	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	deployIfNotExists	<a href="#">1.2.0 ↗</a>
<a href="#">There should be more than one owner assigned to your subscription ↗</a>	It is recommended to designate more than one subscription owner in order to have administrator access redundancy.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Least Privilege (AC-6)

ID: IRS 1075 9.3.1.6

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">A maximum of 3 owners should be designated for your subscription ↗</a>	It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a	modify	<a href="#">1.2.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">assignments on virtual machines with no identities</a>	prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .		
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	1.2.0
<a href="#">Audit Windows machines missing any of specified members in the Administrators group</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if the local Administrators group does not contain one or more members that are listed in the policy parameter.	auditIfNotExists	1.0.0
<a href="#">Audit Windows machines that have the specified members in the Administrators group</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if the local Administrators group contains one or more of the members listed in the policy parameter.	auditIfNotExists	1.0.0
<a href="#">Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs</a>	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	1.2.0
<a href="#">There should be more than one</a>	It is recommended to designate more than one subscription owner in order to have	AuditIfNotExists, Disabled	3.0.0

Name assigned to your subscription (Azure portal)	Description	Effect(s)	Version (GitHub)
---------------------------------------------------	-------------	-----------	------------------

## Risk Assessment

### Vulnerability Scanning (RA-5)

ID: IRS 1075 9.3.14.3

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗</a>	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗</a>	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">SQL databases should have vulnerability findings resolved ↗</a>	Monitor vulnerability assessment scan results and recommendations for how to remediate database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">4.1.0 ↗</a>
<a href="#">Vulnerabilities in security configuration on your machines should be remediated ↗</a>	Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>

## System and Communications Protection

### Protection of Information at Rest (SC-28)

ID: IRS 1075 9.3.16.15

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Transparent Data Encryption on SQL databases should be enabled ↗	Transparent data encryption should be enabled to protect data-at-rest and meet compliance requirements	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources ↗	<p>By default, a virtual machine's OS and data disks are encrypted-at-rest using platform-managed keys. Temp disks, data caches and data flowing between compute and storage aren't encrypted.</p> <p>Disregard this recommendation if: 1. using encryption-at-host, or 2. server-side encryption on Managed Disks meets your security requirements.</p> <p>Learn more in: Server-side encryption of Azure Disk Storage: <a href="https://aka.ms/disksse">https://aka.ms/disksse</a>, ↗ Different disk encryption offerings: <a href="https://aka.ms/diskencryptioncomparison">https://aka.ms/diskencryptioncomparison</a> ↗</p>	AuditIfNotExists, Disabled	<a href="#">2.0.3 ↗</a>

## Denial of Service Protection (SC-5)

ID: IRS 1075 9.3.16.4

  Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure DDoS Protection Standard should be enabled ↗	DDoS protection standard should be enabled for all virtual networks with a subnet that is part of an application gateway with a public IP.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Boundary Protection (SC-7)

ID: IRS 1075 9.3.16.5

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adaptive application controls for defining safe applications should be enabled on your machines ↗	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
All network ports should be restricted on network security groups associated to your virtual machine ↗	Azure Security Center has identified some of your network security groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Storage accounts should restrict network access ↗	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges	Audit, Deny, Disabled	<a href="#">1.1.1 ↗</a>

## Transmission Confidentiality and Integrity (SC-8)

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	modify	<a href="#">1.2.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	modify	<a href="#">1.2.0 ↗</a>
<a href="#">App Service apps should only be accessible over HTTPS ↗</a>	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	<a href="#">4.0.0 ↗</a>
<a href="#">Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs ↗</a>	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	deployIfNotExists	<a href="#">1.2.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Function apps should only be accessible over HTTPS ↗	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	5.0.0 ↗
Only secure connections to your Azure Cache for Redis should be enabled ↗	Audit enabling of only connections via SSL to Azure Cache for Redis. Use of secure connections ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking	Audit, Deny, Disabled	1.0.0 ↗
Secure transfer to storage accounts should be enabled ↗	Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking	Audit, Deny, Disabled	2.0.0 ↗
Windows machines should be configured to use secure communication protocols ↗	To protect the privacy of information communicated over the Internet, your machines should use the latest version of the industry-standard cryptographic protocol, Transport Layer Security (TLS). TLS secures communications over a network by encrypting a connection between machines.	AuditIfNotExists, Disabled	3.0.1 ↗

## System and Information Integrity

### Flaw Remediation (SI-2)

ID: IRS 1075 9.3.17.2

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
SQL databases should have vulnerability findings resolved ↴	Monitor vulnerability assessment scan results and recommendations for how to remediate database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">4.1.0 ↴</a>
System updates should be installed on your machines ↴	Missing security system updates on your servers will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>
Vulnerabilities in security configuration on your machines should be remediated ↴	Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↴</a>

## Malicious Code Protection (SI-3)

ID: IRS 1075 9.3.17.3

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Monitor missing Endpoint Protection in Azure Security Center ↴	Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↴</a>

## Information System Monitoring (SI-4)

ID: IRS 1075 9.3.17.4

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Log Analytics Extension should be enabled for listed virtual machine images ↴	Reports virtual machines as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	<a href="#">2.0.1-preview ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	2.0.1 ↗
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↗
Log Analytics extension should be enabled in virtual machine scale sets for listed virtual machine images ↗	Reports virtual machine scale sets as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	2.0.1 ↗
Virtual machines should be connected to a specified workspace ↗	Reports virtual machines as non-compliant if they aren't logging to the Log Analytics workspace specified in the policy/initiative assignment.	AuditIfNotExists, Disabled	1.1.0 ↗

## Awareness and Training

### Audit Generation (AU-12)

ID: IRS 1075 9.3.3.11

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Log Analytics Extension should be enabled for listed virtual machine images ↗	Reports virtual machines as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	2.0.1-preview ↗
Audit diagnostic setting for selected resource types ↗	Audit diagnostic setting for selected resource types. Be sure to select only resource types which support diagnostics settings.	AuditIfNotExists	2.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Auditing on SQL server should be enabled ↗</a>	Auditing on your SQL Server should be enabled to track database activities across all databases on the server and save them in an audit log.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗</a>	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗</a>	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Log Analytics extension should be enabled in virtual machine scale sets for listed virtual machine images ↗</a>	Reports virtual machine scale sets as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Virtual machines should be connected to a specified workspace ↗</a>	Reports virtual machines as non-compliant if they aren't logging to the Log Analytics workspace specified in the policy/initiative assignment.	AuditIfNotExists, Disabled	<a href="#">1.1.0 ↗</a>

## Content of Audit Records (AU-3)

ID: IRS 1075 9.3.3.3

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Preview]: Log Analytics Extension should be enabled for listed virtual machine images ↗</a>	Reports virtual machines as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	<a href="#">2.0.1-preview ↗</a>
<a href="#">Log Analytics extension should be enabled in virtual machine scale sets</a>	Reports virtual machine scale sets as non-compliant if the virtual machine image is not in the list	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
for listed virtual machine images ↗	defined and the extension is not installed.		
Virtual machines should be connected to a specified workspace ↗	Reports virtual machines as non-compliant if they aren't logging to the Log Analytics workspace specified in the policy/initiative assignment.	AuditIfNotExists, Disabled	1.1.0 ↗

## Response to Audit Processing Failures (AU-5)

ID: IRS 1075 9.3.3.5

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Audit diagnostic setting for selected resource types ↗	Audit diagnostic setting for selected resource types. Be sure to select only resource types which support diagnostics settings.	AuditIfNotExists	2.0.1 ↗
Auditing on SQL server should be enabled ↗	Auditing on your SQL Server should be enabled to track database activities across all databases on the server and save them in an audit log.	AuditIfNotExists, Disabled	2.0.0 ↗
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	2.0.1 ↗
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↗

## Audit Review, Analysis, and Reporting (AU-6)

ID: IRS 1075 9.3.3.6

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Log Analytics Extension should be enabled for listed virtual machine images ↗	Reports virtual machines as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	2.0.1- preview ↗
Log Analytics extension should be enabled in virtual machine scale sets for listed virtual machine images ↗	Reports virtual machine scale sets as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	2.0.1 ↗
Virtual machines should be connected to a specified workspace ↗	Reports virtual machines as non-compliant if they aren't logging to the Log Analytics workspace specified in the policy/initiative assignment.	AuditIfNotExists, Disabled	1.1.0 ↗

## Configuration Management

### User-Installed Software (CM-11)

ID: IRS 1075 9.3.5.11

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adaptive application controls for defining safe applications should be enabled on your machines ↗	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	3.0.0 ↗

### Least Functionality (CM-7)

ID: IRS 1075 9.3.5.7

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications should be enabled on your machines ↗</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Contingency Planning

### Alternate Processing Site (CP-7)

ID: IRS 1075 9.3.6.6

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit virtual machines without disaster recovery configured ↗</a>	Audit virtual machines which do not have disaster recovery configured. To learn more about disaster recovery, visit <a href="https://aka.ms/asr-doc">https://aka.ms/asr-doc ↗</a> .	auditIfNotExists	<a href="#">1.0.0 ↗</a>

## Identification and Authentication

### Identification and Authentication (Organizational Users) (IA-2)

ID: IRS 1075 9.3.7.2

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Accounts with owner permissions on Azure resources should be MFA enabled ↗	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
Accounts with read permissions on Azure resources should be MFA enabled ↗	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
Accounts with write permissions on Azure resources should be MFA enabled ↗	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

## Authenticator Management (IA-5)

ID: IRS 1075 9.3.7.5

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗ .	modify	<a href="#">1.2.0 ↗</a>
Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines	modify	<a href="#">1.2.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .		
Audit Linux machines that do not have the passwd file permissions set to 0644	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Linux machines that do not have the passwd file permissions set to 0644	AuditIfNotExists, Disabled	1.3.0
Audit Linux machines that have accounts without passwords	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Linux machines that have accounts without passwords	AuditIfNotExists, Disabled	1.3.0
Audit Windows machines that allow re-use of the passwords after the specified number of unique passwords	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that allow re-use of the passwords after the specified number of unique passwords. Default value for unique passwords is 24	AuditIfNotExists, Disabled	1.1.0
Audit Windows machines that do not have the maximum password age set to specified number of days	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not have the maximum password age set to specified number of days. Default value for maximum password age is 70 days	AuditIfNotExists, Disabled	1.1.0
Audit Windows machines that do not have the minimum password age set to specified number of days	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not have the minimum password age set to specified number of days. Default value for minimum password age is 1 day	AuditIfNotExists, Disabled	1.1.0
Audit Windows machines that do not have the password complexity setting enabled	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not have the password complexity setting enabled	AuditIfNotExists, Disabled	1.0.0

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit Windows machines that do not restrict the minimum password length to specified number of characters ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Windows machines that do not restrict the minimum password length to specified number of characters. Default value for minimum password length is 14 characters	AuditIfNotExists, Disabled	<a href="#">1.1.0</a> ↗
Audit Windows machines that do not store passwords using reversible encryption ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Windows machines that do not store passwords using reversible encryption	AuditIfNotExists, Disabled	<a href="#">1.0.0</a> ↗
Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↗	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	deployIfNotExists	<a href="#">1.3.0</a> ↗
Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs ↗	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	deployIfNotExists	<a href="#">1.2.0</a> ↗

## Next steps

Additional articles about Azure Policy:

- [Regulatory Compliance](#) overview.
- See the [initiative definition structure](#).

- Review other examples at [Azure Policy samples](#).
- Review [Understanding policy effects](#).
- Learn how to [remediate non-compliant resources](#).

# Details of the ISO 27001:2013 (Azure Government) Regulatory Compliance built-in initiative

Article • 01/02/2024

The following article details how the Azure Policy Regulatory Compliance built-in initiative definition maps to **compliance domains** and **controls** in ISO 27001:2013 (Azure Government). For more information about this compliance standard, see [ISO 27001:2013](#). To understand *Ownership*, see [Azure Policy policy definition](#) and [Shared responsibility in the cloud](#).

The following mappings are to the ISO 27001:2013 controls. Many of the controls are implemented with an [Azure Policy](#) initiative definition. To review the complete initiative definition, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the ISO 27001:2013 Regulatory Compliance built-in initiative definition.

This built-in initiative is deployed as part of the [ISO 27001:2013 blueprint sample](#).

## Important

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policy definitions themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between compliance domains, controls, and Azure Policy definitions for this compliance standard may change over time. To view the change history, see the [GitHub Commit History](#).

## Cryptography

### Policy on the use of cryptographic controls

ID: ISO 27001:2013 A.10.1.1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	<a href="#">1.2.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	<a href="#">1.2.0 ↗</a>
<a href="#">App Service apps should only be accessible over HTTPS ↗</a>	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	<a href="#">4.0.0 ↗</a>
<a href="#">Audit Windows machines that do not store passwords using reversible encryption ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not store passwords using reversible encryption	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Automation account variables should be encrypted ↗</a>	It is important to enable encryption of Automation account variable assets when storing sensitive data	Audit, Deny, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define cryptographic use ↗</a>	CMA_0120 - Define cryptographic use	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs <a href="#">🔗</a>	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> <a href="#">🔗</a> .	deployIfNotExists	1.2.0 <a href="#">🔗</a>
Document and distribute a privacy policy <a href="#">🔗</a>	CMA_0188 - Document and distribute a privacy policy	Manual, Disabled	1.1.0 <a href="#">🔗</a>
Function apps should only be accessible over HTTPS <a href="#">🔗</a>	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	5.0.0 <a href="#">🔗</a>
Implement privacy notice delivery methods <a href="#">🔗</a>	CMA_0324 - Implement privacy notice delivery methods	Manual, Disabled	1.1.0 <a href="#">🔗</a>
Only secure connections to your Azure Cache for Redis should be enabled <a href="#">🔗</a>	Audit enabling of only connections via SSL to Azure Cache for Redis. Use of secure connections ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking	Audit, Deny, Disabled	1.0.0 <a href="#">🔗</a>
Provide privacy notice <a href="#">🔗</a>	CMA_0414 - Provide privacy notice	Manual, Disabled	1.1.0 <a href="#">🔗</a>
Restrict communications <a href="#">🔗</a>	CMA_0449 - Restrict communications	Manual, Disabled	1.1.0 <a href="#">🔗</a>
Review and update system and communications protection policies and procedures <a href="#">🔗</a>	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	1.1.0 <a href="#">🔗</a>
Secure transfer to storage accounts should be enabled <a href="#">🔗</a>	Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures	Audit, Deny, Disabled	2.0.0 <a href="#">🔗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking		
Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign ↗	Service Fabric provides three levels of protection (None, Sign and EncryptAndSign) for node-to-node communication using a primary cluster certificate. Set the protection level to ensure that all node-to-node messages are encrypted and digitally signed	Audit, Deny, Disabled	1.1.0 ↗
Transparent Data Encryption on SQL databases should be enabled ↗	Transparent data encryption should be enabled to protect data-at-rest and meet compliance requirements	AuditIfNotExists, Disabled	2.0.0 ↗
Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources ↗	By default, a virtual machine's OS and data disks are encrypted-at-rest using platform-managed keys. Temp disks, data caches and data flowing between compute and storage aren't encrypted. Disregard this recommendation if: 1. using encryption-at-host, or 2. server-side encryption on Managed Disks meets your security requirements. Learn more in: Server-side encryption of Azure Disk Storage: <a href="https://aka.ms/disksse">https://aka.ms/disksse</a> , ↗ Different disk encryption offerings: <a href="https://aka.ms/diskencryptioncomparison">https://aka.ms/diskencryptioncomparison</a> ↗	AuditIfNotExists, Disabled	2.0.3 ↗

## Key Management

ID: ISO 27001:2013 A.10.1.2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define a physical key management process ↗	CMA_0115 - Define a physical key management process	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define cryptographic use ↗	CMA_0120 - Define cryptographic use	Manual, Disabled	1.1.0 ↗
Define organizational requirements for cryptographic key management ↗	CMA_0123 - Define organizational requirements for cryptographic key management	Manual, Disabled	1.1.0 ↗
Determine assertion requirements ↗	CMA_0136 - Determine assertion requirements	Manual, Disabled	1.1.0 ↗
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Establish a password policy ↗	CMA_0256 - Establish a password policy	Manual, Disabled	1.1.0 ↗
Identify actions allowed without authentication ↗	CMA_0295 - Identify actions allowed without authentication	Manual, Disabled	1.1.0 ↗
Identify and authenticate non-organizational users ↗	CMA_C1346 - Identify and authenticate non-organizational users	Manual, Disabled	1.1.0 ↗
Implement parameters for memorized secret verifiers ↗	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	1.1.0 ↗
Issue public key certificates ↗	CMA_0347 - Issue public key certificates	Manual, Disabled	1.1.0 ↗
Manage symmetric cryptographic keys ↗	CMA_0367 - Manage symmetric cryptographic keys	Manual, Disabled	1.1.0 ↗
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	1.1.0 ↗
Restrict access to private keys ↗	CMA_0445 - Restrict access to private keys	Manual, Disabled	1.1.0 ↗
Review and update system and communications protection policies and procedures ↗	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	1.1.0 ↗
Terminate customer controlled account credentials ↗	CMA_C1022 - Terminate customer controlled account credentials	Manual, Disabled	1.1.0 ↗

## Physical And Environmental Security

# Physical security perimeter

ID: ISO 27001:2013 A.11.1.1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define a physical key management process ↗</a>	CMA_0115 - Define a physical key management process	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and maintain an asset inventory ↗</a>	CMA_0266 - Establish and maintain an asset inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Install an alarm system ↗</a>	CMA_0338 - Install an alarm system	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage a secure surveillance camera system ↗</a>	CMA_0354 - Manage a secure surveillance camera system	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update physical and environmental policies and procedures ↗</a>	CMA_C1446 - Review and update physical and environmental policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Physical entry controls

ID: ISO 27001:2013 A.11.1.2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual,	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
			Disabled
Define a physical key management process ↗	CMA_0115 - Define a physical key management process	Manual, Disabled	1.1.0 ↗
Designate personnel to supervise unauthorized maintenance activities ↗	CMA_C1422 - Designate personnel to supervise unauthorized maintenance activities	Manual, Disabled	1.1.0 ↗
Establish and maintain an asset inventory ↗	CMA_0266 - Establish and maintain an asset inventory	Manual, Disabled	1.1.0 ↗
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	1.1.0 ↗
Maintain list of authorized remote maintenance personnel ↗	CMA_C1420 - Maintain list of authorized remote maintenance personnel	Manual, Disabled	1.1.0 ↗
Manage maintenance personnel ↗	CMA_C1421 - Manage maintenance personnel	Manual, Disabled	1.1.0 ↗
Manage the input, output, processing, and storage of data ↗	CMA_0369 - Manage the input, output, processing, and storage of data	Manual, Disabled	1.1.0 ↗

## Securing offices, rooms and facilities

ID: ISO 27001:2013 A.11.1.3 Ownership: Shared

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
			Disabled
Adopt biometric authentication mechanisms ↗	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	1.1.0 ↗
Control physical access ↗	CMA_0081 - Control physical access	Manual, Disabled	1.1.0 ↗
Define a physical key management process ↗	CMA_0115 - Define a physical key management process	Manual, Disabled	1.1.0 ↗
Establish and maintain an asset	CMA_0266 - Establish and maintain	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
inventory ↗	an asset inventory	Disabled	
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	1.1.0 ↗

## Protecting against external and environmental threats

ID: ISO 27001:2013 A.11.1.4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Create separate alternate and primary storage sites ↗	CMA_C1269 - Create separate alternate and primary storage sites	Manual, Disabled	1.1.0 ↗
Ensure alternate storage site safeguards are equivalent to primary site ↗	CMA_C1268 - Ensure alternate storage site safeguards are equivalent to primary site	Manual, Disabled	1.1.0 ↗
Ensure information system fails in known state ↗	CMA_C1662 - Ensure information system fails in known state	Manual, Disabled	1.1.0 ↗
Establish alternate storage site to store and retrieve backup information ↗	CMA_C1267 - Establish alternate storage site to store and retrieve backup information	Manual, Disabled	1.1.0 ↗
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗
Identify and mitigate potential issues at alternate storage site ↗	CMA_C1271 - Identify and mitigate potential issues at alternate storage site	Manual, Disabled	1.1.0 ↗
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	1.1.0 ↗
Install an alarm system ↗	CMA_0338 - Install an alarm system	Manual, Disabled	1.1.0 ↗
Plan for continuance of essential business functions ↗	CMA_C1255 - Plan for continuance of essential business functions	Manual, Disabled	1.1.0 ↗

## Working in secure areas

ID: ISO 27001:2013 A.11.1.5 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update contingency planning policies and procedures ↗	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update physical and environmental policies and procedures ↗	CMA_C1446 - Review and update physical and environmental policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Delivering and loading areas

ID: ISO 27001:2013 A.11.1.6 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
Adopt biometric authentication mechanisms ↗	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Define requirements for managing assets ↗	CMA_0125 - Define requirements for managing assets	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Install an alarm system ↗	CMA_0338 - Install an alarm system	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage a secure surveillance camera system ↗	CMA_0354 - Manage a secure surveillance camera system	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Equipment sitting and protection

ID: ISO 27001:2013 A.11.2.1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Supporting utilities

ID: ISO 27001:2013 A.11.2.2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ automatic emergency lighting ↗	CMA_0209 - Employ automatic emergency lighting	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish requirements for internet service providers ↗	CMA_0278 - Establish requirements for internet service providers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Cabling security

ID: ISO 27001:2013 A.11.2.3 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adopt biometric authentication mechanisms ↗	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Control physical access ↗	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Manage the input, output, processing, and storage of data ↗	CMA_0369 - Manage the input, output, processing, and storage of data	Manual, Disabled	1.1.0 ↗

## Equipment maintenance

ID: ISO 27001:2013 A.11.2.4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate remote maintenance activities ↗	CMA_C1402 - Automate remote maintenance activities	Manual, Disabled	1.1.0 ↗
Control maintenance and repair activities ↗	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	1.1.0 ↗
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	Manual, Disabled	1.1.0 ↗
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Manage nonlocal maintenance and diagnostic activities ↗	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	1.1.0 ↗
Produce complete records of remote maintenance activities ↗	CMA_C1403 - Produce complete records of remote maintenance activities	Manual, Disabled	1.1.0 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗
Provide timely maintenance support ↗	CMA_C1425 - Provide timely maintenance support	Manual, Disabled	1.1.0 ↗

## Removal of assets

ID: ISO 27001:2013 A.11.2.5 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Control maintenance and repair activities ↗	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Define requirements for managing assets ↗	CMA_0125 - Define requirements for managing assets	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage nonlocal maintenance and diagnostic activities ↗	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security of equipment and assets off-premises

ID: ISO 27001:2013 A.11.2.6 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define mobile device requirements ↗	CMA_0122 - Define mobile device requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Ensure security safeguards not needed when the individuals return ↗	CMA_C1183 - Ensure security safeguards not needed when the individuals return	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish terms and conditions for accessing resources ↗	CMA_C1076 - Establish terms and conditions for accessing resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish terms and conditions for processing resources ↗	CMA_C1077 - Establish terms and conditions for processing resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure alternate work sites ↗	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Not allow for information systems to accompany with individuals ↗	CMA_C1182 - Not allow for information systems to accompany with individuals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify security controls for external information systems ↗	CMA_0541 - Verify security controls for external information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Secure disposal or re-use of equipment

ID: ISO 27001:2013 A.11.2.7 Ownership: Shared

[+] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adhere to retention periods defined ↗	CMA_0004 - Adhere to retention periods defined	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform disposition review ↗	CMA_0391 - Perform disposition review	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify personal data is deleted at the end of processing ↗	CMA_0540 - Verify personal data is deleted at the end of processing	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Unattended user equipment

ID: ISO 27001:2013 A.11.2.8 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Terminate user session automatically ↗	CMA_C1054 - Terminate user session automatically	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Clear desk and clear screen policy

ID: ISO 27001:2013 A.11.2.9 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Operations Security

### Documented operating procedures

ID: ISO 27001:2013 A.12.1.1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop audit and accountability policies and procedures ↗	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	1.1.0 ↗
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	1.1.0 ↗
Distribute information system documentation ↗	CMA_C1584 - Distribute information system documentation	Manual, Disabled	1.1.0 ↗
Document customer-defined actions ↗	CMA_C1582 - Document customer-defined actions	Manual, Disabled	1.1.0 ↗
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	1.1.0 ↗
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗
Obtain Admin documentation ↗	CMA_C1580 - Obtain Admin documentation	Manual, Disabled	1.1.0 ↗
Obtain user security function documentation ↗	CMA_C1581 - Obtain user security function documentation	Manual, Disabled	1.1.0 ↗
Protect administrator and user documentation ↗	CMA_C1583 - Protect administrator and user documentation	Manual, Disabled	1.1.0 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗
Review access control policies and procedures ↗	CMA_0457 - Review access control policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update configuration management policies and	CMA_C1175 - Review and update configuration management policies	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
procedures ↗	and procedures		
Review and update contingency planning policies and procedures ↗	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update identification and authentication policies and procedures ↗	CMA_C1299 - Review and update identification and authentication policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update incident response policies and procedures ↗	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update information integrity policies and procedures ↗	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update media protection policies and procedures ↗	CMA_C1427 - Review and update media protection policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update personnel security policies and procedures ↗	CMA_C1507 - Review and update personnel security policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update physical and environmental policies and procedures ↗	CMA_C1446 - Review and update physical and environmental policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update planning policies and procedures ↗	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update risk assessment policies and procedures ↗	CMA_C1537 - Review and update risk assessment policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update system and communications protection policies and procedures ↗	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update system and services acquisition policies and procedures ↗	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update system maintenance policies and procedures ↗	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review security assessment and authorization policies and procedures ↗	CMA_C1143 - Review security assessment and authorization policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Change management

ID: ISO 27001:2013 A.12.1.2 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Address coding vulnerabilities ↗	CMA_0003 - Address coding vulnerabilities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate approval request for proposed changes ↗	CMA_C1192 - Automate approval request for proposed changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate implementation of approved change notifications ↗	CMA_C1196 - Automate implementation of approved change notifications	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate process to document implemented changes ↗	CMA_C1195 - Automate process to document implemented changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate process to highlight unreviewed change proposals ↗	CMA_C1193 - Automate process to highlight unreviewed change proposals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate process to prohibit implementation of unapproved changes ↗	CMA_C1194 - Automate process to prohibit implementation of unapproved changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate proposed documented changes ↗	CMA_C1191 - Automate proposed documented changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and document application security requirements ↗	CMA_0148 - Develop and document application security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop and maintain a vulnerability management standard ↗	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a secure software development program ↗	CMA_0259 - Establish a secure software development program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Install an alarm system ↗	CMA_0338 - Install an alarm system	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage nonlocal maintenance and diagnostic activities ↗	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Remediate information system	CMA_0427 - Remediate information	Manual,	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">flaws ↗</a>	system flaws	Disabled	
<a href="#">Require developers to document approved changes and potential impact ↗</a>	CMA_C1597 - Require developers to document approved changes and potential impact	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require developers to implement only approved changes ↗</a>	CMA_C1596 - Require developers to implement only approved changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require developers to manage change integrity ↗</a>	CMA_C1595 - Require developers to manage change integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Capacity management

ID: ISO 27001:2013 A.12.1.3 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Conduct capacity planning ↗</a>	CMA_C1252 - Conduct capacity planning	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Govern and monitor audit processing activities ↗</a>	CMA_0289 - Govern and monitor audit processing activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Separation of development, testing and operational environments

ID: ISO 27001:2013 A.12.1.4 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Conduct a security impact analysis ↗</a>	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Ensure there are no unencrypted static authenticators ↗</a>	CMA_C1340 - Ensure there are no unencrypted static authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗
Implement controls to protect PII ↗	CMA_C1839 - Implement controls to protect PII	Manual, Disabled	1.1.0 ↗
Incorporate security and data privacy practices in research processing ↗	CMA_0331 - Incorporate security and data privacy practices in research processing	Manual, Disabled	1.1.0 ↗
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	1.1.0 ↗
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗

## Controls against malware

ID: ISO 27001:2013 A.12.2.1 Ownership: Shared

↔ Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↗
Control maintenance and repair activities ↗	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	1.1.0 ↗
Manage gateways ↗	CMA_0363 - Manage gateways	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Manage nonlocal maintenance and diagnostic activities ↗	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	1.1.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Provide periodic security awareness training ↗	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 ↗
Provide security training for new users ↗	CMA_0419 - Provide security training for new users	Manual, Disabled	1.1.0 ↗
Provide updated security awareness training ↗	CMA_C1090 - Provide updated security awareness training	Manual, Disabled	1.1.0 ↗
Review malware detections report weekly ↗	CMA_0475 - Review malware detections report weekly	Manual, Disabled	1.1.0 ↗
Review threat protection status weekly ↗	CMA_0479 - Review threat protection status weekly	Manual, Disabled	1.1.0 ↗
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗

## Information backup

ID: ISO 27001:2013 A.12.3.1 Ownership: Shared

[\[+\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adhere to retention periods defined ↗	CMA_0004 - Adhere to retention periods defined	Manual, Disabled	1.1.0 ↗
Conduct backup of information system documentation ↗	CMA_C1289 - Conduct backup of information system documentation	Manual, Disabled	1.1.0 ↗
Create separate alternate and primary storage sites ↗	CMA_C1269 - Create separate alternate and primary storage sites	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure information system fails in known state ↗	CMA_C1662 - Ensure information system fails in known state	Manual, Disabled	1.1.0 ↗
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗
Establish backup policies and procedures ↗	CMA_0268 - Establish backup policies and procedures	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Implement transaction based recovery ↗	CMA_C1296 - Implement transaction based recovery	Manual, Disabled	1.1.0 ↗
Perform disposition review ↗	CMA_0391 - Perform disposition review	Manual, Disabled	1.1.0 ↗
Plan for continuance of essential business functions ↗	CMA_C1255 - Plan for continuance of essential business functions	Manual, Disabled	1.1.0 ↗
Separately store backup information ↗	CMA_C1293 - Separately store backup information	Manual, Disabled	1.1.0 ↗
Transfer backup information to an alternate storage site ↗	CMA_C1294 - Transfer backup information to an alternate storage site	Manual, Disabled	1.1.0 ↗
Verify personal data is deleted at the end of processing ↗	CMA_0540 - Verify personal data is deleted at the end of processing	Manual, Disabled	1.1.0 ↗

## Event Logging

ID: ISO 27001:2013 A.12.4.1 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Log Analytics Extension should be enabled for listed virtual machine images ↗	Reports virtual machines as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	2.0.1- preview ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adhere to retention periods defined ↴	CMA_0004 - Adhere to retention periods defined	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Alert personnel of information spillage ↴	CMA_0007 - Alert personnel of information spillage	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Audit diagnostic setting for selected resource types ↴	Audit diagnostic setting for selected resource types. Be sure to select only resource types which support diagnostics settings.	AuditIfNotExists	<a href="#">2.0.1 ↗</a>
Audit privileged functions ↴	CMA_0019 - Audit privileged functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Audit user account status ↴	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Auditing on SQL server should be enabled ↴	Auditing on your SQL Server should be enabled to track database activities across all databases on the server and save them in an audit log.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
Authorize, monitor, and control voip ↴	CMA_0025 - Authorize, monitor, and control voip	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate account management ↴	CMA_0026 - Automate account management	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Check for privacy and security compliance before establishing internal connections ↴	CMA_0053 - Check for privacy and security compliance before establishing internal connections	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Conduct a full text analysis of logged privileged commands ↴	CMA_0056 - Conduct a full text analysis of logged privileged commands	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Configure Azure Audit capabilities ↴	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	<a href="#">1.1.1 ↗</a>
Correlate audit records ↴	CMA_0087 - Correlate audit records	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Dependency agent should be enabled for listed virtual machine images ↴	Reports virtual machines as non-compliant if the virtual machine image is not in the list defined and the agent is not installed. The list of	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	OS images is updated over time as support is updated.		
Dependency agent should be enabled in virtual machine scale sets for listed virtual machine images ↗	Reports virtual machine scale sets as non-compliant if the virtual machine image is not in the list defined and the agent is not installed. The list of OS images is updated over time as support is updated.	AuditIfNotExists, Disabled	2.0.0 ↗
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Discover any indicators of compromise ↗	CMA_C1702 - Discover any indicators of compromise	Manual, Disabled	1.1.0 ↗
Document the legal basis for processing personal information ↗	CMA_0206 - Document the legal basis for processing personal information	Manual, Disabled	1.1.0 ↗
Enforce and audit access restrictions ↗	CMA_C1203 - Enforce and audit access restrictions	Manual, Disabled	1.1.0 ↗
Establish requirements for audit review and reporting ↗	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	1.1.0 ↗
Implement methods for consumer requests ↗	CMA_0319 - Implement methods for consumer requests	Manual, Disabled	1.1.0 ↗
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	1.1.0 ↗
Integrate audit review, analysis, and reporting ↗	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	1.1.0 ↗
Integrate cloud app security with a siem ↗	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	1.1.0 ↗
Log Analytics extension should be enabled in virtual machine scale sets for listed virtual machine images ↗	Reports virtual machine scale sets as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	2.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Manage gateways ↗	CMA_0363 - Manage gateways	Manual, Disabled	1.1.0 ↗
Manage system and admin accounts ↗	CMA_0368 - Manage system and admin accounts	Manual, Disabled	1.1.0 ↗
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	1.1.0 ↗
Monitor account activity ↗	CMA_0377 - Monitor account activity	Manual, Disabled	1.1.0 ↗
Monitor privileged role assignment ↗	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	1.1.0 ↗
Notify when account is not needed ↗	CMA_0383 - Notify when account is not needed	Manual, Disabled	1.1.0 ↗
Obtain legal opinion for monitoring system activities ↗	CMA_C1688 - Obtain legal opinion for monitoring system activities	Manual, Disabled	1.1.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Provide monitoring information as needed ↗	CMA_C1689 - Provide monitoring information as needed	Manual, Disabled	1.1.0 ↗
Publish access procedures in SORNs ↗	CMA_C1848 - Publish access procedures in SORNs	Manual, Disabled	1.1.0 ↗
Publish rules and regulations accessing Privacy Act records ↗	CMA_C1847 - Publish rules and regulations accessing Privacy Act records	Manual, Disabled	1.1.0 ↗
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	1.1.0 ↗
Retain security policies and procedures ↗	CMA_0454 - Retain security policies and procedures	Manual, Disabled	1.1.0 ↗
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	1.1.0 ↗
Review account provisioning logs ↗	CMA_0460 - Review account provisioning logs	Manual, Disabled	1.1.0 ↗
Review administrator assignments weekly ↗	CMA_0461 - Review administrator assignments weekly	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update the events defined in AU-02 ↗	CMA_C1106 - Review and update the events defined in AU-02	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review audit data ↗	CMA_0466 - Review audit data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review changes for any unauthorized changes ↗	CMA_C1204 - Review changes for any unauthorized changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review cloud identity report overview ↗	CMA_0468 - Review cloud identity report overview	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review controlled folder access events ↗	CMA_0471 - Review controlled folder access events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review file and folder activity ↗	CMA_0473 - Review file and folder activity	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review role group changes weekly ↗	CMA_0476 - Review role group changes weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Set automated notifications for new and trending cloud applications in your organization ↗	CMA_0495 - Set automated notifications for new and trending cloud applications in your organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Protection of log information

ID: ISO 27001:2013 A.12.4.2 Ownership: Shared

 [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adhere to retention periods defined ↗	CMA_0004 - Adhere to retention periods defined	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Define the duties of processors ↗	CMA_0127 - Define the duties of processors	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enable dual or joint authorization ↗	CMA_0226 - Enable dual or joint authorization	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform disposition review ↗	CMA_0391 - Perform disposition review	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect audit information ↗	CMA_0401 - Protect audit information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Record disclosures of PII to third parties ↗	CMA_0422 - Record disclosures of PII to third parties	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Train staff on PII sharing and its consequences ↗	CMA_C1871 - Train staff on PII sharing and its consequences	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify personal data is deleted at the end of processing ↗	CMA_0540 - Verify personal data is deleted at the end of processing	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Administrator and operator logs

ID: ISO 27001:2013 A.12.4.3 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Log Analytics Extension should be enabled for listed virtual machine images ↗	Reports virtual machines as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	<a href="#">2.0.1- preview ↗</a>
Audit diagnostic setting for selected resource types ↗	Audit diagnostic setting for selected resource types. Be sure to select only resource types which support diagnostics settings.	AuditIfNotExists	<a href="#">2.0.1 ↗</a>
Audit privileged functions ↗	CMA_0019 - Audit privileged functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Auditing on SQL server should be enabled ↗</a>	Auditing on your SQL Server should be enabled to track database activities across all databases on the server and save them in an audit log.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Authorize, monitor, and control voip ↗</a>	CMA_0025 - Authorize, monitor, and control voip	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate account management ↗</a>	CMA_0026 - Automate account management	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Check for privacy and security compliance before establishing internal connections ↗</a>	CMA_0053 - Check for privacy and security compliance before establishing internal connections	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct a full text analysis of logged privileged commands ↗</a>	CMA_0056 - Conduct a full text analysis of logged privileged commands	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Dependency agent should be enabled for listed virtual machine images ↗</a>	Reports virtual machines as non-compliant if the virtual machine image is not in the list defined and the agent is not installed. The list of OS images is updated over time as support is updated.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Dependency agent should be enabled in virtual machine scale sets for listed virtual machine images ↗</a>	Reports virtual machine scale sets as non-compliant if the virtual machine image is not in the list defined and the agent is not installed. The list of OS images is updated over time as support is updated.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Determine auditable events ↗</a>	CMA_0137 - Determine auditable events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enable dual or joint authorization ↗</a>	CMA_0226 - Enable dual or joint authorization	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement system boundary protection ↗</a>	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Log Analytics extension should be enabled in virtual machine scale sets for listed virtual machine images ↗	Reports virtual machine scale sets as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	2.0.1 ↗
Manage gateways ↗	CMA_0363 - Manage gateways	Manual, Disabled	1.1.0 ↗
Manage system and admin accounts ↗	CMA_0368 - Manage system and admin accounts	Manual, Disabled	1.1.0 ↗
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	1.1.0 ↗
Monitor account activity ↗	CMA_0377 - Monitor account activity	Manual, Disabled	1.1.0 ↗
Monitor privileged role assignment ↗	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	1.1.0 ↗
Notify when account is not needed ↗	CMA_0383 - Notify when account is not needed	Manual, Disabled	1.1.0 ↗
Obtain legal opinion for monitoring system activities ↗	CMA_C1688 - Obtain legal opinion for monitoring system activities	Manual, Disabled	1.1.0 ↗
Protect audit information ↗	CMA_0401 - Protect audit information	Manual, Disabled	1.1.0 ↗
Provide monitoring information as needed ↗	CMA_C1689 - Provide monitoring information as needed	Manual, Disabled	1.1.0 ↗
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	1.1.0 ↗
Review audit data ↗	CMA_0466 - Review audit data	Manual, Disabled	1.1.0 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	1.1.0 ↗
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↗

# Clock Synchronization

ID: ISO 27001:2013 A.12.4.4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Log Analytics Extension should be enabled for listed virtual machine images ↗	Reports virtual machines as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	2.0.1-preview ↗
Audit diagnostic setting for selected resource types ↗	Audit diagnostic setting for selected resource types. Be sure to select only resource types which support diagnostics settings.	AuditIfNotExists	2.0.1 ↗
Auditing on SQL server should be enabled ↗	Auditing on your SQL Server should be enabled to track database activities across all databases on the server and save them in an audit log.	AuditIfNotExists, Disabled	2.0.0 ↗
Compile Audit records into system wide audit ↗	CMA_C1140 - Compile Audit records into system wide audit	Manual, Disabled	1.1.0 ↗
Dependency agent should be enabled for listed virtual machine images ↗	Reports virtual machines as non-compliant if the virtual machine image is not in the list defined and the agent is not installed. The list of OS images is updated over time as support is updated.	AuditIfNotExists, Disabled	2.0.0 ↗
Dependency agent should be enabled in virtual machine scale sets for listed virtual machine images ↗	Reports virtual machine scale sets as non-compliant if the virtual machine image is not in the list defined and the agent is not installed. The list of OS images is updated over time as support is updated.	AuditIfNotExists, Disabled	2.0.0 ↗
Log Analytics extension should be enabled in virtual machine scale sets for listed virtual machine images ↗	Reports virtual machine scale sets as non-compliant if the virtual machine image is not in the list defined and the extension is not installed.	AuditIfNotExists, Disabled	2.0.1 ↗
Use system clocks for audit records ↗	CMA_0535 - Use system clocks for audit records	Manual, Disabled	1.1.0 ↗

# Installation of software on operational systems

ID: ISO 27001:2013 A.12.5.1 Ownership: Shared

  Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adaptive application controls for defining safe applications should be enabled on your machines ↗	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Automate approval request for proposed changes ↗	CMA_C1192 - Automate approval request for proposed changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate implementation of approved change notifications ↗	CMA_C1196 - Automate implementation of approved change notifications	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate process to document implemented changes ↗	CMA_C1195 - Automate process to document implemented changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate process to highlight unreviewed change proposals ↗	CMA_C1193 - Automate process to highlight unreviewed change proposals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate process to prohibit implementation of unapproved changes ↗	CMA_C1194 - Automate process to prohibit implementation of unapproved changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate proposed documented changes ↗	CMA_C1191 - Automate proposed documented changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop and maintain a vulnerability management standard ↗	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Govern compliance of cloud service providers ↗	CMA_0290 - Govern compliance of cloud service providers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Management of technical vulnerabilities

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct Risk Assessment ↗	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Conduct risk assessment and distribute its results ↗	CMA_C1544 - Conduct risk assessment and distribute its results	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Conduct risk assessment and document its results ↗	CMA_C1542 - Conduct risk assessment and document its results	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Incorporate flaw remediation into configuration management ↗	CMA_C1671 - Incorporate flaw remediation into configuration management	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor missing Endpoint Protection in Azure Security Center ↗	Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Select additional testing for security control assessments ↗	CMA_C1149 - Select additional testing for security control assessments	Manual, Disabled	<a href="#">1.1.0 ↗</a>
SQL databases should have vulnerability findings resolved ↗	Monitor vulnerability assessment scan results and recommendations for how to remediate database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">4.1.0 ↗</a>
System updates should be installed on your machines ↗	Missing security system updates on your servers will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Vulnerabilities in security configuration on your	Servers which do not satisfy the configured baseline will be	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
machines should be remediated ↗	monitored by Azure Security Center as recommendations		

## Restrictions on software installation

ID: ISO 27001:2013 A.12.6.2 Ownership: Shared

[ ] Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Adaptive application controls for defining safe applications should be enabled on your machines ↗	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Automate approval request for proposed changes ↗	CMA_C1192 - Automate approval request for proposed changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate implementation of approved change notifications ↗	CMA_C1196 - Automate implementation of approved change notifications	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate process to document implemented changes ↗	CMA_C1195 - Automate process to document implemented changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate process to highlight unreviewed change proposals ↗	CMA_C1193 - Automate process to highlight unreviewed change proposals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate process to prohibit implementation of unapproved changes ↗	CMA_C1194 - Automate process to prohibit implementation of unapproved changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate proposed documented changes ↗	CMA_C1191 - Automate proposed documented changes	Manual, Disabled	1.1.0 ↗
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Develop and maintain a vulnerability management standard ↗	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	1.1.0 ↗
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗
Govern compliance of cloud service providers ↗	CMA_0290 - Govern compliance of cloud service providers	Manual, Disabled	1.1.0 ↗
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	1.1.0 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	1.1.0 ↗
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">View and configure system diagnostic data ↗</a>	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information systems audit controls

ID: ISO 27001:2013 A.12.7.1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ independent team for penetration testing ↗</a>	CMA_C1171 - Employ independent team for penetration testing	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Communications Security

### Network controls

ID: ISO 27001:2013 A.13.1.1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">All network ports should be restricted on network security groups associated to your virtual machine ↗</a>	Azure Security Center has identified some of your network security groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Authorize access to security functions and information ↗</a>	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize and manage access ↗	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Authorize remote access ↗	CMA_0024 - Authorize remote access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Configure workstations to check for digital certificates ↗	CMA_0073 - Configure workstations to check for digital certificates	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document and implement wireless access guidelines ↗	CMA_0190 - Document and implement wireless access guidelines	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document mobility training ↗	CMA_0191 - Document mobility training	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document remote access guidelines ↗	CMA_0196 - Document remote access guidelines	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Employ boundary protection to isolate information systems ↗	CMA_C1639 - Employ boundary protection to isolate information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce logical access ↗	CMA_0245 - Enforce logical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish firewall and router configuration standards ↗	CMA_0272 - Establish firewall and router configuration standards	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish network segmentation for card holder data environment ↗	CMA_0273 - Establish network segmentation for card holder data environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish terms and conditions for accessing resources ↗	CMA_C1076 - Establish terms and conditions for accessing resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish terms and conditions for	CMA_C1077 - Establish terms and conditions for processing resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">processing resources ↗</a>			
Identify and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Identify and manage downstream information exchanges ↗	CMA_0298 - Identify and manage downstream information exchanges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement a fault tolerant name/address service ↗	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement controls to secure alternate work sites ↗	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement managed interface for each external service ↗	CMA_C1626 - Implement managed interface for each external service	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify users of system logon or access ↗	CMA_0382 - Notify users of system logon or access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Prevent split tunneling for remote devices ↗	CMA_C1632 - Prevent split tunneling for remote devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Produce, control and distribute asymmetric cryptographic keys ↗	CMA_C1646 - Produce, control and distribute asymmetric cryptographic keys	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect wireless access ↗	CMA_0411 - Protect wireless access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide secure name and address resolution services ↴	CMA_0416 - Provide secure name and address resolution services	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Reauthenticate or terminate a user session ↴	CMA_0421 - Reauthenticate or terminate a user session	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Require approval for account creation ↴	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review user groups and applications with access to sensitive data ↴	CMA_0481 - Review user groups and applications with access to sensitive data	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Secure the interface to external systems ↴	CMA_0491 - Secure the interface to external systems	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Separate user and information system management functionality ↴	CMA_0493 - Separate user and information system management functionality	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Storage accounts should restrict network access ↴	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges	Audit, Deny, Disabled	<a href="#">1.1.1 ↴</a>
Use dedicated machines for administrative tasks ↴	CMA_0527 - Use dedicated machines for administrative tasks	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Verify security controls for external information systems ↴	CMA_0541 - Verify security controls for external information systems	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Security of network services

ID: ISO 27001:2013 A.13.1.2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adopt biometric authentication mechanisms ↗	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Define and document government oversight ↗	CMA_C1587 - Define and document government oversight	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish electronic signature and certificate requirements ↗	CMA_0271 - Establish electronic signature and certificate requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish firewall and router configuration standards ↗	CMA_0272 - Establish firewall and router configuration standards	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish network segmentation for card holder data environment ↗	CMA_0273 - Establish network segmentation for card holder data environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Identify and manage downstream information exchanges ↗	CMA_0298 - Identify and manage downstream information exchanges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Prevent split tunneling for remote devices ↗	CMA_C1632 - Prevent split tunneling for remote devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require external service providers to comply with security requirements ↗	CMA_C1586 - Require external service providers to comply with security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require interconnection security agreements ↗	CMA_C1151 - Require interconnection security agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review cloud service provider's compliance with policies and agreements ↗	CMA_0469 - Review cloud service provider's compliance with policies and agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Undergo independent security review ↗</a>	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update interconnection security agreements ↗</a>	CMA_0519 - Update interconnection security agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Segregation of networks

ID: ISO 27001:2013 A.13.1.3 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authorize remote access ↗</a>	CMA_0024 - Authorize remote access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Configure workstations to check for digital certificates ↗</a>	CMA_0073 - Configure workstations to check for digital certificates	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Control information flow ↗</a>	CMA_0079 - Control information flow	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ boundary protection to isolate information systems ↗</a>	CMA_C1639 - Employ boundary protection to isolate information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ flow control mechanisms of encrypted information ↗</a>	CMA_0211 - Employ flow control mechanisms of encrypted information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish firewall and router configuration standards ↗</a>	CMA_0272 - Establish firewall and router configuration standards	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish network segmentation for card holder data environment ↗</a>	CMA_0273 - Establish network segmentation for card holder data environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify and manage downstream information exchanges ↗</a>	CMA_0298 - Identify and manage downstream information exchanges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement a fault tolerant name/address service ↗</a>	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement managed interface for each external service ↗	CMA_C1626 - Implement managed interface for each external service	Manual, Disabled	1.1.0 ↗
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	1.1.0 ↗
Information flow control using security policy filters ↗	CMA_C1029 - Information flow control using security policy filters	Manual, Disabled	1.1.0 ↗
Prevent split tunneling for remote devices ↗	CMA_C1632 - Prevent split tunneling for remote devices	Manual, Disabled	1.1.0 ↗
Provide secure name and address resolution services ↗	CMA_0416 - Provide secure name and address resolution services	Manual, Disabled	1.1.0 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	Manual, Disabled	1.1.0 ↗
Separate user and information system management functionality ↗	CMA_0493 - Separate user and information system management functionality	Manual, Disabled	1.1.0 ↗
Use dedicated machines for administrative tasks ↗	CMA_0527 - Use dedicated machines for administrative tasks	Manual, Disabled	1.1.0 ↗

## Information transfer policies and procedures

ID: ISO 27001:2013 A.13.2.1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize remote access ↗	CMA_0024 - Authorize remote access	Manual, Disabled	1.1.0 ↗
Configure workstations to check for digital certificates ↗	CMA_0073 - Configure workstations to check for digital certificates	Manual, Disabled	1.1.0 ↗
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define mobile device requirements ↗	CMA_0122 - Define mobile device requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document and implement wireless access guidelines ↗	CMA_0190 - Document and implement wireless access guidelines	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document mobility training ↗	CMA_0191 - Document mobility training	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document remote access guidelines ↗	CMA_0196 - Document remote access guidelines	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Employ flow control mechanisms of encrypted information ↗	CMA_0211 - Employ flow control mechanisms of encrypted information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish firewall and router configuration standards ↗	CMA_0272 - Establish firewall and router configuration standards	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish network segmentation for card holder data environment ↗	CMA_0273 - Establish network segmentation for card holder data environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish terms and conditions for accessing resources ↗	CMA_C1076 - Establish terms and conditions for accessing resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish terms and conditions for processing resources ↗	CMA_C1077 - Establish terms and conditions for processing resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Explicitly notify use of collaborative computing devices ↗	CMA_C1649 - Explicitly notify use of collaborative computing devices	Manual, Disabled	<a href="#">1.1.1 ↗</a>
Identify and manage downstream information exchanges ↗	CMA_0298 - Identify and manage downstream information exchanges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement a fault tolerant name/address service ↗	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure alternate work sites ↴	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement managed interface for each external service ↴	CMA_C1626 - Implement managed interface for each external service	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement system boundary protection ↴	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Information flow control using security policy filters ↴	CMA_C1029 - Information flow control using security policy filters	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Only secure connections to your Azure Cache for Redis should be enabled ↴	Audit enabling of only connections via SSL to Azure Cache for Redis. Use of secure connections ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
Produce, control and distribute asymmetric cryptographic keys ↴	CMA_C1646 - Produce, control and distribute asymmetric cryptographic keys	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Prohibit remote activation of collaborative computing devices ↴	CMA_C1648 - Prohibit remote activation of collaborative computing devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect data in transit using encryption ↴	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect passwords with encryption ↴	CMA_0408 - Protect passwords with encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect wireless access ↴	CMA_0411 - Protect wireless access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Provide privacy training ↴	CMA_0415 - Provide privacy training	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Provide secure name and address resolution services ↴	CMA_0416 - Provide secure name and address resolution services	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require interconnection	CMA_C1151 - Require interconnection security agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal) Secure the interface to external systems ↴	CMA_0491 - Secure the interface to external systems	Manual, Disabled	(GitHub) <a href="#">1.1.0 ↴</a>
Secure transfer to storage accounts should be enabled ↴	Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking	Audit, Deny, Disabled	<a href="#">2.0.0 ↴</a>
Update interconnection security agreements ↴	CMA_0519 - Update interconnection security agreements	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Verify security controls for external information systems ↴	CMA_0541 - Verify security controls for external information systems	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Agreements on information transfer

ID: ISO 27001:2013 A.13.2.2 Ownership: Shared

[\[ \]](#) Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Define and document government oversight ↴	CMA_C1587 - Define and document government oversight	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Document personnel acceptance of privacy requirements ↴	CMA_0193 - Document personnel acceptance of privacy requirements	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Identify external service providers ↴	CMA_C1591 - Identify external service providers	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Implement privacy notice delivery methods ↴	CMA_0324 - Implement privacy notice delivery methods	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Obtain consent prior to collection or processing of personal data ↴	CMA_0385 - Obtain consent prior to collection or processing of personal data	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Provide privacy notice ↴	CMA_0414 - Provide privacy notice	Manual, Disabled	<a href="#">1.1.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require external service providers to comply with security requirements ↗	CMA_C1586 - Require external service providers to comply with security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require interconnection security agreements ↗	CMA_C1151 - Require interconnection security agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review cloud service provider's compliance with policies and agreements ↗	CMA_0469 - Review cloud service provider's compliance with policies and agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update interconnection security agreements ↗	CMA_0519 - Update interconnection security agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Electronic messaging

ID: ISO 27001:2013 A.13.2.3 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure workstations to check for digital certificates ↗	CMA_0073 - Configure workstations to check for digital certificates	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish firewall and router configuration standards ↗	CMA_0272 - Establish firewall and router configuration standards	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish network segmentation for card holder data environment ↗	CMA_0273 - Establish network segmentation for card holder data environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Identify and manage downstream information exchanges ↗	CMA_0298 - Identify and manage downstream information exchanges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement a fault tolerant name/address service ↗	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Produce, control and distribute asymmetric cryptographic keys ↗	CMA_C1646 - Produce, control and distribute asymmetric cryptographic keys	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Provide secure name and address resolution services ↗	CMA_0416 - Provide secure name and address resolution services	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Confidentiality or non-disclosure agreements

ID: ISO 27001:2013 A.13.2.4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop acceptable use policies and procedures ↗	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop security safeguards ↗	CMA_0161 - Develop security safeguards	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document organizational access agreements ↗	CMA_0192 - Document organizational access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce rules of behavior and access agreements ↗	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Ensure access agreements are signed or resigned timely ↗	CMA_C1528 - Ensure access agreements are signed or resigned timely	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require users to sign access agreement ↗	CMA_0440 - Require users to sign access agreement	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update organizational access agreements ↗	CMA_0520 - Update organizational access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## System Acquisition, Development And Maintenance

### Information security requirements analysis and specification

ID: ISO 27001:2013 A.14.1.1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define information security roles and responsibilities ↗	CMA_C1565 - Define information security roles and responsibilities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Determine supplier contract obligations ↗	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop a concept of operations (CONOPS) ↗	CMA_0141 - Develop a concept of operations (CONOPS)	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop SSP that meets criteria ↗	CMA_C1492 - Develop SSP that meets criteria	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document acquisition contract acceptance criteria ↗	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document protection of personal data in acquisition contracts ↗	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document protection of security information in acquisition contracts ↗	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document requirements for the use of shared data in contracts ↗	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security assurance requirements in acquisition contracts ↗	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security documentation requirements in acquisition contract ↗	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security functional requirements in acquisition contracts ↗	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document the protection of cardholder data in third party contracts ↗	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	1.1.0 ↗
Identify external service providers ↗	CMA_C1591 - Identify external service providers	Manual, Disabled	1.1.0 ↗
Identify individuals with security roles and responsibilities ↗	CMA_C1566 - Identify individuals with security roles and responsibilities	Manual, Disabled	1.1.1 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗
Integrate risk management process into SDLC ↗	CMA_C1567 - Integrate risk management process into SDLC	Manual, Disabled	1.1.0 ↗
Review and update the information security architecture ↗	CMA_C1504 - Review and update the information security architecture	Manual, Disabled	1.1.0 ↗
Review development process, standards and tools ↗	CMA_C1610 - Review development process, standards and tools	Manual, Disabled	1.1.0 ↗

## Securing application services on public networks

ID: ISO 27001:2013 A.14.1.2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adopt biometric authentication mechanisms ↗	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	1.1.0 ↗
Authorize access to security functions and information ↗	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	1.1.0 ↗
Authorize and manage access ↗	CMA_0023 - Authorize and manage access	Manual, Disabled	1.1.0 ↗
Authorize remote access ↗	CMA_0024 - Authorize remote access	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure workstations to check for digital certificates ↗	CMA_0073 - Configure workstations to check for digital certificates	Manual, Disabled	1.1.0 ↗
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	1.1.0 ↗
Define cryptographic use ↗	CMA_0120 - Define cryptographic use	Manual, Disabled	1.1.0 ↗
Document mobility training ↗	CMA_0191 - Document mobility training	Manual, Disabled	1.1.0 ↗
Document remote access guidelines ↗	CMA_0196 - Document remote access guidelines	Manual, Disabled	1.1.0 ↗
Employ flow control mechanisms of encrypted information ↗	CMA_0211 - Employ flow control mechanisms of encrypted information	Manual, Disabled	1.1.0 ↗
Enforce logical access ↗	CMA_0245 - Enforce logical access	Manual, Disabled	1.1.0 ↗
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	1.1.0 ↗
Enforce user uniqueness ↗	CMA_0250 - Enforce user uniqueness	Manual, Disabled	1.1.0 ↗
Establish firewall and router configuration standards ↗	CMA_0272 - Establish firewall and router configuration standards	Manual, Disabled	1.1.0 ↗
Establish network segmentation for card holder data environment ↗	CMA_0273 - Establish network segmentation for card holder data environment	Manual, Disabled	1.1.0 ↗
Identify and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	1.1.0 ↗
Identify and authenticate non-organizational users ↗	CMA_C1346 - Identify and authenticate non-organizational users	Manual, Disabled	1.1.0 ↗
Identify and manage downstream information exchanges ↗	CMA_0298 - Identify and manage downstream information exchanges	Manual, Disabled	1.1.0 ↗
Implement a fault tolerant name/address service ↗	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement controls to secure alternate work sites ↗	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Information flow control using security policy filters ↗	CMA_C1029 - Information flow control using security policy filters	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify users of system logon or access ↗	CMA_0382 - Notify users of system logon or access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Produce, control and distribute asymmetric cryptographic keys ↗	CMA_C1646 - Produce, control and distribute asymmetric cryptographic keys	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Provide secure name and address resolution services ↗	CMA_0416 - Provide secure name and address resolution services	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review user groups and applications with access to sensitive data ↗	CMA_0481 - Review user groups and applications with access to sensitive data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Support personal verification credentials issued by legal authorities ↗	CMA_0507 - Support personal verification credentials issued by legal authorities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Protecting application services transactions

ID: ISO 27001:2013 A.14.1.3 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authorize access to security functions and information ↗</a>	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Authorize and manage access ↗</a>	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Authorize remote access ↗</a>	CMA_0024 - Authorize remote access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Configure workstations to check for digital certificates ↗</a>	CMA_0073 - Configure workstations to check for digital certificates	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Control information flow ↗</a>	CMA_0079 - Control information flow	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define cryptographic use ↗</a>	CMA_0120 - Define cryptographic use	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ boundary protection to isolate information systems ↗</a>	CMA_C1639 - Employ boundary protection to isolate information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ flow control mechanisms of encrypted information ↗</a>	CMA_0211 - Employ flow control mechanisms of encrypted information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce logical access ↗</a>	CMA_0245 - Enforce logical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce mandatory and discretionary access control policies ↗</a>	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce user uniqueness ↗</a>	CMA_0250 - Enforce user uniqueness	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish firewall and router configuration standards ↗</a>	CMA_0272 - Establish firewall and router configuration standards	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish network segmentation for card holder data environment ↗</a>	CMA_0273 - Establish network segmentation for card holder data environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify and authenticate non-organizational users ↗</a>	CMA_C1346 - Identify and authenticate non-organizational users	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Identify and manage downstream information exchanges ↗</a>	CMA_0298 - Identify and manage downstream information exchanges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement a fault tolerant name/address service ↗</a>	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement system boundary protection ↗</a>	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Information flow control using security policy filters ↗</a>	CMA_C1029 - Information flow control using security policy filters	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Prevent split tunneling for remote devices ↗</a>	CMA_C1632 - Prevent split tunneling for remote devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Produce, control and distribute asymmetric cryptographic keys ↗</a>	CMA_C1646 - Produce, control and distribute asymmetric cryptographic keys	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Protect data in transit using encryption ↗</a>	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Protect passwords with encryption ↗</a>	CMA_0408 - Protect passwords with encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Provide secure name and address resolution services ↗</a>	CMA_0416 - Provide secure name and address resolution services	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require approval for account creation ↗</a>	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review user groups and applications with access to sensitive data ↗</a>	CMA_0481 - Review user groups and applications with access to sensitive data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Secure the interface to external systems ↗</a>	CMA_0491 - Secure the interface to external systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Separate user and information system management functionality ↗</a>	CMA_0493 - Separate user and information system management functionality	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Support personal verification credentials issued by legal authorities ↗</a>	CMA_0507 - Support personal verification credentials issued by legal authorities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Use dedicated machines for administrative tasks ↗</a>	CMA_0527 - Use dedicated machines for administrative tasks	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Secure development policy

ID: ISO 27001:2013 A.14.2.1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define information security roles and responsibilities ↗	CMA_C1565 - Define information security roles and responsibilities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Identify individuals with security roles and responsibilities ↗	CMA_C1566 - Identify individuals with security roles and responsibilities	Manual, Disabled	<a href="#">1.1.1 ↗</a>
Integrate risk management process into SDLC ↗	CMA_C1567 - Integrate risk management process into SDLC	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to build security architecture ↗	CMA_C1612 - Require developers to build security architecture	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to describe accurate security functionality ↗	CMA_C1613 - Require developers to describe accurate security functionality	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to provide unified security protection approach ↗	CMA_C1614 - Require developers to provide unified security protection approach	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review development process, standards and tools ↗	CMA_C1610 - Review development process, standards and tools	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# System change control procedures

ID: ISO 27001:2013 A.14.2.2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Address coding vulnerabilities ↗	CMA_0003 - Address coding vulnerabilities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate approval request for proposed changes ↗	CMA_C1192 - Automate approval request for proposed changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate implementation of approved change notifications ↗	CMA_C1196 - Automate implementation of approved change notifications	Manual, Disabled	1.1.0 ↗
Automate process to document implemented changes ↗	CMA_C1195 - Automate process to document implemented changes	Manual, Disabled	1.1.0 ↗
Automate process to highlight unreviewed change proposals ↗	CMA_C1193 - Automate process to highlight unreviewed change proposals	Manual, Disabled	1.1.0 ↗
Automate process to prohibit implementation of unapproved changes ↗	CMA_C1194 - Automate process to prohibit implementation of unapproved changes	Manual, Disabled	1.1.0 ↗
Automate proposed documented changes ↗	CMA_C1191 - Automate proposed documented changes	Manual, Disabled	1.1.0 ↗
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Develop and document application security requirements ↗	CMA_0148 - Develop and document application security requirements	Manual, Disabled	1.1.0 ↗
Develop and maintain a vulnerability management standard ↗	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	1.1.0 ↗
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↗
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗
Establish a secure software development program ↗	CMA_0259 - Establish a secure software development program	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Incorporate flaw remediation into configuration management ↗	CMA_C1671 - Incorporate flaw remediation into configuration management	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to document approved changes and potential impact ↗	CMA_C1597 - Require developers to document approved changes and potential impact	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to implement only approved changes ↗	CMA_C1596 - Require developers to implement only approved changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to manage change integrity ↗	CMA_C1595 - Require developers to manage change integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Technical review of applications after operating platform changes

ID: ISO 27001:2013 A.14.2.3 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate approval request for proposed changes ↗	CMA_C1192 - Automate approval request for proposed changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate implementation of approved change notifications ↗	CMA_C1196 - Automate implementation of approved change notifications	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate process to document implemented changes ↗	CMA_C1195 - Automate process to document implemented changes	Manual, Disabled	1.1.0 ↗
Automate process to highlight unreviewed change proposals ↗	CMA_C1193 - Automate process to highlight unreviewed change proposals	Manual, Disabled	1.1.0 ↗
Automate process to prohibit implementation of unapproved changes ↗	CMA_C1194 - Automate process to prohibit implementation of unapproved changes	Manual, Disabled	1.1.0 ↗
Automate proposed documented changes ↗	CMA_C1191 - Automate proposed documented changes	Manual, Disabled	1.1.0 ↗
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Develop and maintain a vulnerability management standard ↗	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	1.1.0 ↗
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗
Incorporate flaw remediation into configuration management ↗	CMA_C1671 - Incorporate flaw remediation into configuration management	Manual, Disabled	1.1.0 ↗
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	1.1.0 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	1.1.0 ↗
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	scans	Disabled	
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗

## Restrictions on changes to software packages

ID: ISO 27001:2013 A.14.2.4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Address coding vulnerabilities ↗	CMA_0003 - Address coding vulnerabilities	Manual, Disabled	1.1.0 ↗
Automate approval request for proposed changes ↗	CMA_C1192 - Automate approval request for proposed changes	Manual, Disabled	1.1.0 ↗
Automate implementation of approved change notifications ↗	CMA_C1196 - Automate implementation of approved change notifications	Manual, Disabled	1.1.0 ↗
Automate process to document implemented changes ↗	CMA_C1195 - Automate process to document implemented changes	Manual, Disabled	1.1.0 ↗
Automate process to highlight unreviewed change proposals ↗	CMA_C1193 - Automate process to highlight unreviewed change proposals	Manual, Disabled	1.1.0 ↗
Automate process to prohibit implementation of unapproved changes ↗	CMA_C1194 - Automate process to prohibit implementation of unapproved changes	Manual, Disabled	1.1.0 ↗
Automate proposed documented changes ↗	CMA_C1191 - Automate proposed documented changes	Manual, Disabled	1.1.0 ↗
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Develop and document application security requirements ↗	CMA_0148 - Develop and document application security requirements	Manual, Disabled	1.1.0 ↗
Develop and maintain a vulnerability management	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
standard ↗			
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↗
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗
Establish a secure software development program ↗	CMA_0259 - Establish a secure software development program	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	1.1.0 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	1.1.0 ↗
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗
Require developers to document approved changes and potential impact ↗	CMA_C1597 - Require developers to document approved changes and potential impact	Manual, Disabled	1.1.0 ↗
Require developers to implement only approved changes ↗	CMA_C1596 - Require developers to implement only approved changes	Manual, Disabled	1.1.0 ↗
Require developers to manage change integrity ↗	CMA_C1595 - Require developers to manage change integrity	Manual, Disabled	1.1.0 ↗

## Secure system engineering principles

ID: ISO 27001:2013 A.14.2.5 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform information input validation ↗	CMA_C1723 - Perform information input validation	Manual, Disabled	1.1.0 ↗
Require developers to build security architecture ↗	CMA_C1612 - Require developers to build security architecture	Manual, Disabled	1.1.0 ↗
Require developers to describe accurate security functionality ↗	CMA_C1613 - Require developers to describe accurate security functionality	Manual, Disabled	1.1.0 ↗
Require developers to provide unified security protection approach ↗	CMA_C1614 - Require developers to provide unified security protection approach	Manual, Disabled	1.1.0 ↗
Review development process, standards and tools ↗	CMA_C1610 - Review development process, standards and tools	Manual, Disabled	1.1.0 ↗

## Secure development environment

ID: ISO 27001:2013 A.14.2.6 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Define information security roles and responsibilities ↗	CMA_C1565 - Define information security roles and responsibilities	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗
Identify individuals with security roles and responsibilities ↗	CMA_C1566 - Identify individuals with security roles and	Manual, Disabled	1.1.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	responsibilities		
Integrate risk management process into SDLC ↗	CMA_C1567 - Integrate risk management process into SDLC	Manual, Disabled	1.1.0 ↗
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	1.1.0 ↗
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗

## Outsourced development

ID: ISO 27001:2013 A.14.2.7 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Address coding vulnerabilities ↗	CMA_0003 - Address coding vulnerabilities	Manual, Disabled	1.1.0 ↗
Assess risk in third party relationships ↗	CMA_0014 - Assess risk in third party relationships	Manual, Disabled	1.1.0 ↗
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Define requirements for supplying goods and services ↗	CMA_0126 - Define requirements for supplying goods and services	Manual, Disabled	1.1.0 ↗
Determine supplier contract obligations ↗	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	1.1.0 ↗
Develop and document application security requirements ↗	CMA_0148 - Develop and document application security requirements	Manual, Disabled	1.1.0 ↗
Document acquisition contract acceptance criteria ↗	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document protection of personal data in acquisition contracts ↗	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document protection of security information in acquisition contracts ↗	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document requirements for the use of shared data in contracts ↗	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	1.1.0 ↗
Document security assurance requirements in acquisition contracts ↗	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document security documentation requirements in acquisition contract ↗	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	1.1.0 ↗
Document security functional requirements in acquisition contracts ↗	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the protection of cardholder data in third party contracts ↗	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	1.1.0 ↗
Establish a secure software development program ↗	CMA_0259 - Establish a secure software development program	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗
Establish policies for supply chain risk management ↗	CMA_0275 - Establish policies for supply chain risk management	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to document approved changes and potential impact ↗	CMA_C1597 - Require developers to document approved changes and potential impact	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to implement only approved changes ↗	CMA_C1596 - Require developers to implement only approved changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to manage change integrity ↗	CMA_C1595 - Require developers to manage change integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to produce evidence of security assessment plan execution ↗	CMA_C1602 - Require developers to produce evidence of security assessment plan execution	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## System security testing

ID: ISO 27001:2013 A.14.2.8 Ownership: Shared

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess Security Controls ↗	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Deliver security assessment results ↗	CMA_C1147 - Deliver security assessment results	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop security assessment plan ↗	CMA_C1144 - Develop security assessment plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Ensure there are no unencrypted static authenticators ↗	CMA_C1340 - Ensure there are no unencrypted static authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Produce Security Assessment report ↗	CMA_C1146 - Produce Security Assessment report	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to produce evidence of security assessment plan execution ↗	CMA_C1602 - Require developers to produce evidence of security assessment plan execution	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## System acceptance testing

ID: ISO 27001:2013 A.14.2.9 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign an authorizing official (AO) ↗	CMA_C1158 - Assign an authorizing official (AO)	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Determine supplier contract obligations ↗	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document acquisition contract acceptance criteria ↗	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document protection of personal data in acquisition contracts ↗	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document protection of security information in acquisition contracts ↗	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document requirements for the use of shared data in contracts ↗	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security assurance requirements in acquisition contracts ↗	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security documentation requirements in acquisition contract ↗	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	1.1.0 ↗
Document security functional requirements in acquisition contracts ↗	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the protection of cardholder data in third party contracts ↗	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	1.1.0 ↗
Ensure resources are authorized ↗	CMA_C1159 - Ensure resources are authorized	Manual, Disabled	1.1.0 ↗
Ensure there are no unencrypted static authenticators ↗	CMA_C1340 - Ensure there are no unencrypted static authenticators	Manual, Disabled	1.1.0 ↗

## Protection of test data

ID: ISO 27001:2013 A.14.3.1 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adhere to retention periods defined ↗	CMA_0004 - Adhere to retention periods defined	Manual, Disabled	1.1.0 ↗
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Ensure there are no unencrypted static authenticators ↗	CMA_C1340 - Ensure there are no unencrypted static authenticators	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform disposition review ↗	CMA_0391 - Perform disposition review	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify personal data is deleted at the end of processing ↗	CMA_0540 - Verify personal data is deleted at the end of processing	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Supplier Relationships

### Information security policy for supplier relationships

ID: ISO 27001:2013 A.15.1.1 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess risk in third party relationships ↗	CMA_0014 - Assess risk in third party relationships	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Define requirements for supplying goods and services ↗	CMA_0126 - Define requirements for supplying goods and services	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Determine supplier contract obligations ↗	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish policies for supply chain risk management ↗	CMA_0275 - Establish policies for supply chain risk management	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update personnel security policies and procedures ↗	CMA_C1507 - Review and update personnel security policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update system and services acquisition policies and procedures ↗	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	1.1.0 ↗

## Addressing security within supplier agreement

ID: ISO 27001:2013 A.15.1.2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess risk in third party relationships ↗	CMA_0014 - Assess risk in third party relationships	Manual, Disabled	1.1.0 ↗
Check for privacy and security compliance before establishing internal connections ↗	CMA_0053 - Check for privacy and security compliance before establishing internal connections	Manual, Disabled	1.1.0 ↗
Define requirements for supplying goods and services ↗	CMA_0126 - Define requirements for supplying goods and services	Manual, Disabled	1.1.0 ↗
Determine supplier contract obligations ↗	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	1.1.0 ↗
Develop acceptable use policies and procedures ↗	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	1.1.0 ↗
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	1.1.0 ↗
Document acquisition contract acceptance criteria ↗	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	1.1.0 ↗
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	Manual, Disabled	1.1.0 ↗
Document protection of personal data in acquisition contracts ↗	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Document protection of security information in acquisition contracts ↗</a>	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document requirements for the use of shared data in contracts ↗</a>	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security assurance requirements in acquisition contracts ↗</a>	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security documentation requirements in acquisition contract ↗</a>	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security functional requirements in acquisition contracts ↗</a>	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security strength requirements in acquisition contracts ↗</a>	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document the information system environment in acquisition contracts ↗</a>	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document the protection of cardholder data in third party contracts ↗</a>	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce rules of behavior and access agreements ↗</a>	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish policies for supply chain risk management ↗</a>	CMA_0275 - Establish policies for supply chain risk management	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify external service providers ↗</a>	CMA_C1591 - Identify external service providers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Prohibit unfair practices ↗</a>	CMA_0396 - Prohibit unfair practices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and sign revised rules of behavior ↗</a>	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update rules of behavior and</a>	CMA_0521 - Update rules of	Manual,	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">access agreements ↗</a>	behavior and access agreements	Disabled	
<a href="#">Update rules of behavior and access agreements every 3 years ↗</a>	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information and communication technology supply chain

ID: ISO 27001:2013 A.15.1.3 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess risk in third party relationships ↗</a>	CMA_0014 - Assess risk in third party relationships	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define requirements for supplying goods and services ↗</a>	CMA_0126 - Define requirements for supplying goods and services	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Determine supplier contract obligations ↗</a>	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish policies for supply chain risk management ↗</a>	CMA_0275 - Establish policies for supply chain risk management	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Monitoring and review of supplier services

ID: ISO 27001:2013 A.15.2.1 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define and document government oversight ↗</a>	CMA_C1587 - Define and document government oversight	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require external service providers to comply with security requirements ↗</a>	CMA_C1586 - Require external service providers to comply with security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review cloud service provider's compliance with policies and agreements ↗	CMA_0469 - Review cloud service provider's compliance with policies and agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Managing changes to supplier services

ID: ISO 27001:2013 A.15.2.2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define and document government oversight ↗	CMA_C1587 - Define and document government oversight	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Determine supplier contract obligations ↗	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document acquisition contract acceptance criteria ↗	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document protection of personal data in acquisition contracts ↗	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document protection of security information in acquisition contracts ↗	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document requirements for the use of shared data in contracts ↗	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security assurance requirements in acquisition contracts ↗	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security documentation requirements in acquisition contract ↗	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security functional requirements in acquisition contracts ↗	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the protection of cardholder data in third party contracts ↗	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	1.1.0 ↗
Require external service providers to comply with security requirements ↗	CMA_C1586 - Require external service providers to comply with security requirements	Manual, Disabled	1.1.0 ↗
Review cloud service provider's compliance with policies and agreements ↗	CMA_0469 - Review cloud service provider's compliance with policies and agreements	Manual, Disabled	1.1.0 ↗
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	1.1.0 ↗

## Information Security Incident Management

### Responsibilities and procedures

ID: ISO 27001:2013 A.16.1.1 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess information security events ↗	CMA_0013 - Assess information security events	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗
Maintain data breach records ↗	CMA_0351 - Maintain data breach records	Manual, Disabled	1.1.0 ↗
Maintain incident response plan ↗	CMA_0352 - Maintain incident response plan	Manual, Disabled	1.1.0 ↗
Protect incident response plan ↗	CMA_0405 - Protect incident response plan	Manual, Disabled	1.1.0 ↗
Review and update incident response policies and procedures ↗	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	1.1.0 ↗

## Reporting information security events

ID: ISO 27001:2013 A.16.1.2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Correlate audit records ↗	CMA_0087 - Correlate audit records	Manual, Disabled	1.1.0 ↗
Document security operations ↗	CMA_0202 - Document security operations	Manual, Disabled	1.1.0 ↗
Establish requirements for audit review and reporting ↗	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	1.1.0 ↗
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗
Integrate audit review, analysis, and reporting ↗	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	1.1.0 ↗
Integrate cloud app security with a siem ↗	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	1.1.0 ↗
Report atypical behavior of user accounts ↗	CMA_C1025 - Report atypical behavior of user accounts	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review account provisioning logs ↗</a>	CMA_0460 - Review account provisioning logs	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review administrator assignments weekly ↗</a>	CMA_0461 - Review administrator assignments weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review audit data ↗</a>	CMA_0466 - Review audit data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review cloud identity report overview ↗</a>	CMA_0468 - Review cloud identity report overview	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review controlled folder access events ↗</a>	CMA_0471 - Review controlled folder access events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review file and folder activity ↗</a>	CMA_0473 - Review file and folder activity	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review role group changes weekly ↗</a>	CMA_0476 - Review role group changes weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Reporting information security weaknesses

ID: ISO 27001:2013 A.16.1.3 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Document security operations ↗</a>	CMA_0202 - Document security operations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Incorporate flaw remediation into configuration management ↗</a>	CMA_C1671 - Incorporate flaw remediation into configuration management	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Report atypical behavior of user accounts ↗</a>	CMA_C1025 - Report atypical behavior of user accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Assessment of and decision on information security events

ID: ISO 27001:2013 A.16.1.4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess information security events ↗</a>	CMA_0013 - Assess information security events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Coordinate contingency plans with related plans ↗</a>	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Correlate audit records ↗</a>	CMA_0087 - Correlate audit records	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop an incident response plan ↗</a>	CMA_0145 - Develop an incident response plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop security safeguards ↗</a>	CMA_0161 - Develop security safeguards	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enable network protection ↗</a>	CMA_0238 - Enable network protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Eradicate contaminated information ↗</a>	CMA_0253 - Eradicate contaminated information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish requirements for audit review and reporting ↗</a>	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Execute actions in response to information spills ↗</a>	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement incident handling ↗</a>	CMA_0318 - Implement incident handling	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Integrate audit review, analysis, and reporting ↗</a>	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Integrate cloud app security with a siem ↗</a>	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Maintain incident response plan ↗</a>	CMA_0352 - Maintain incident response plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a trend analysis on</a>	CMA_0389 - Perform a trend analysis	Manual,	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">threats ↗</a>	on threats	Disabled	
<a href="#">Report atypical behavior of user accounts ↗</a>	CMA_C1025 - Report atypical behavior of user accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review account provisioning logs ↗</a>	CMA_0460 - Review account provisioning logs	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review administrator assignments weekly ↗</a>	CMA_0461 - Review administrator assignments weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review audit data ↗</a>	CMA_0466 - Review audit data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review cloud identity report overview ↗</a>	CMA_0468 - Review cloud identity report overview	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review controlled folder access events ↗</a>	CMA_0471 - Review controlled folder access events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review file and folder activity ↗</a>	CMA_0473 - Review file and folder activity	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review role group changes weekly ↗</a>	CMA_0476 - Review role group changes weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">View and investigate restricted users ↗</a>	CMA_0545 - View and investigate restricted users	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Response to information security incidents

ID: ISO 27001:2013 A.16.1.5 Ownership: Shared

[ ] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess information security events ↗</a>	CMA_0013 - Assess information security events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Coordinate contingency plans with related plans ↗</a>	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop an incident response plan ↗</a>	CMA_0145 - Develop an incident response plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop security safeguards ↗	CMA_0161 - Develop security safeguards	Manual, Disabled	1.1.0 ↗
Enable network protection ↗	CMA_0238 - Enable network protection	Manual, Disabled	1.1.0 ↗
Eradicate contaminated information ↗	CMA_0253 - Eradicate contaminated information	Manual, Disabled	1.1.0 ↗
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	1.1.0 ↗
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗
Maintain incident response plan ↗	CMA_0352 - Maintain incident response plan	Manual, Disabled	1.1.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Report atypical behavior of user accounts ↗	CMA_C1025 - Report atypical behavior of user accounts	Manual, Disabled	1.1.0 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

## Learning from information security incidents

ID: ISO 27001:2013 A.16.1.6 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess information security events ↗	CMA_0013 - Assess information security events	Manual, Disabled	1.1.0 ↗
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Develop security safeguards ↗	CMA_0161 - Develop security	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	safeguards	Disabled	
Discover any indicators of compromise 	CMA_C1702 - Discover any indicators of compromise	Manual, Disabled	<a href="#">1.1.0 </a>
Enable network protection 	CMA_0238 - Enable network protection	Manual, Disabled	<a href="#">1.1.0 </a>
Eradicate contaminated information 	CMA_0253 - Eradicate contaminated information	Manual, Disabled	<a href="#">1.1.0 </a>
Execute actions in response to information spills 	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	<a href="#">1.1.0 </a>
Implement incident handling 	CMA_0318 - Implement incident handling	Manual, Disabled	<a href="#">1.1.0 </a>
Maintain incident response plan 	CMA_0352 - Maintain incident response plan	Manual, Disabled	<a href="#">1.1.0 </a>
Perform a trend analysis on threats 	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	<a href="#">1.1.0 </a>
Report atypical behavior of user accounts 	CMA_C1025 - Report atypical behavior of user accounts	Manual, Disabled	<a href="#">1.1.0 </a>
View and investigate restricted users 	CMA_0545 - View and investigate restricted users	Manual, Disabled	<a href="#">1.1.0 </a>

## Collection of evidence

ID: ISO 27001:2013 A.16.1.7 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adhere to retention periods defined 	CMA_0004 - Adhere to retention periods defined	Manual, Disabled	<a href="#">1.1.0 </a>
Check for privacy and security compliance before establishing internal connections 	CMA_0053 - Check for privacy and security compliance before establishing internal connections	Manual, Disabled	<a href="#">1.1.0 </a>
Determine auditable events 	CMA_0137 - Determine auditable events	Manual, Disabled	<a href="#">1.1.0 </a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗
Report atypical behavior of user accounts ↗	CMA_C1025 - Report atypical behavior of user accounts	Manual, Disabled	1.1.0 ↗
Retain security policies and procedures ↗	CMA_0454 - Retain security policies and procedures	Manual, Disabled	1.1.0 ↗
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	1.1.0 ↗

## Information Security Aspects Of Business Continuity Management

### Planning information security continuity

ID: ISO 27001:2013 A.17.1.1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Communicate contingency plan changes ↗	CMA_C1249 - Communicate contingency plan changes	Manual, Disabled	1.1.0 ↗
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	1.1.0 ↗
Develop and document a business continuity and disaster recovery plan ↗	CMA_0146 - Develop and document a business continuity and disaster recovery plan	Manual, Disabled	1.1.0 ↗
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0 ↗
Develop contingency planning policies and procedures ↗	CMA_0156 - Develop contingency planning policies and procedures	Manual, Disabled	1.1.0 ↗
Distribute policies and procedures ↗	CMA_0185 - Distribute policies and procedures	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Plan for resumption of essential business functions ↗	CMA_C1253 - Plan for resumption of essential business functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Resume all mission and business functions ↗	CMA_C1254 - Resume all mission and business functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update contingency planning policies and procedures ↗	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review contingency plan ↗	CMA_C1247 - Review contingency plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update contingency plan ↗	CMA_C1248 - Update contingency plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Implementing information security continuity

ID: ISO 27001:2013 A.17.1.2 Ownership: Shared

[+] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Communicate contingency plan changes ↗	CMA_C1249 - Communicate contingency plan changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Conduct backup of information system documentation ↗	CMA_C1289 - Conduct backup of information system documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Create separate alternate and primary storage sites ↗	CMA_C1269 - Create separate alternate and primary storage sites	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Ensure alternate storage site safeguards are equivalent to primary site ↗	CMA_C1268 - Ensure alternate storage site safeguards are equivalent to primary site	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Ensure information system fails in known state ↗	CMA_C1662 - Ensure information system fails in known state	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish alternate storage site to store and retrieve backup information ↗	CMA_C1267 - Establish alternate storage site to store and retrieve backup information	Manual, Disabled	1.1.0 ↗
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗
Establish backup policies and procedures ↗	CMA_0268 - Establish backup policies and procedures	Manual, Disabled	1.1.0 ↗
Establish requirements for internet service providers ↗	CMA_0278 - Establish requirements for internet service providers	Manual, Disabled	1.1.0 ↗
Identify and mitigate potential issues at alternate storage site ↗	CMA_C1271 - Identify and mitigate potential issues at alternate storage site	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Implement transaction based recovery ↗	CMA_C1296 - Implement transaction based recovery	Manual, Disabled	1.1.0 ↗
Plan for continuance of essential business functions ↗	CMA_C1255 - Plan for continuance of essential business functions	Manual, Disabled	1.1.0 ↗
Plan for resumption of essential business functions ↗	CMA_C1253 - Plan for resumption of essential business functions	Manual, Disabled	1.1.0 ↗
Recover and reconstitute resources after any disruption ↗	CMA_C1295 - Recover and reconstitute resources after any disruption	Manual, Disabled	1.1.1 ↗
Resume all mission and business functions ↗	CMA_C1254 - Resume all mission and business functions	Manual, Disabled	1.1.0 ↗

## Verify, review and evaluate information security continuity

ID: ISO 27001:2013 A.17.1.3 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Initiate contingency plan testing corrective actions ↗	CMA_C1263 - Initiate contingency plan testing corrective actions	Manual, Disabled	1.1.0 ↗
Review the results of contingency plan testing ↗	CMA_C1262 - Review the results of contingency plan testing	Manual, Disabled	1.1.0 ↗
Test the business continuity and disaster recovery plan ↗	CMA_0509 - Test the business continuity and disaster recovery plan	Manual, Disabled	1.1.0 ↗

## Availability of information processing facilities

ID: ISO 27001:2013 A.17.2.1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Communicate contingency plan changes ↗	CMA_C1249 - Communicate contingency plan changes	Manual, Disabled	1.1.0 ↗
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	1.1.0 ↗
Create separate alternate and primary storage sites ↗	CMA_C1269 - Create separate alternate and primary storage sites	Manual, Disabled	1.1.0 ↗
Develop and document a business continuity and disaster recovery plan ↗	CMA_0146 - Develop and document a business continuity and disaster recovery plan	Manual, Disabled	1.1.0 ↗
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0 ↗
Develop contingency planning policies and procedures ↗	CMA_0156 - Develop contingency planning policies and procedures	Manual, Disabled	1.1.0 ↗
Distribute policies and procedures ↗	CMA_0185 - Distribute policies and procedures	Manual, Disabled	1.1.0 ↗
Ensure alternate storage site safeguards are equivalent to primary site ↗	CMA_C1268 - Ensure alternate storage site safeguards are equivalent to primary site	Manual, Disabled	1.1.0 ↗
Ensure information system fails in known state ↗	CMA_C1662 - Ensure information system fails in known state	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish alternate storage site to store and retrieve backup information ↗	CMA_C1267 - Establish alternate storage site to store and retrieve backup information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Identify and mitigate potential issues at alternate storage site ↗	CMA_C1271 - Identify and mitigate potential issues at alternate storage site	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Plan for continuance of essential business functions ↗	CMA_C1255 - Plan for continuance of essential business functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Plan for resumption of essential business functions ↗	CMA_C1253 - Plan for resumption of essential business functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Resume all mission and business functions ↗	CMA_C1254 - Resume all mission and business functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review contingency plan ↗	CMA_C1247 - Review contingency plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update contingency plan ↗	CMA_C1248 - Update contingency plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Compliance

### Identification applicable legislation and contractual requirements

ID: ISO 27001:2013 A.18.1.1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop audit and accountability policies and procedures ↗	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	1.1.0 ↗
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	1.1.0 ↗
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	1.1.0 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	1.1.0 ↗
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗
Protect the information security program plan ↗	CMA_C1732 - Protect the information security program plan	Manual, Disabled	1.1.0 ↗
Review access control policies and procedures ↗	CMA_0457 - Review access control policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update configuration management policies and procedures ↗	CMA_C1175 - Review and update configuration management policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update contingency planning policies and procedures ↗	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update identification and authentication policies and procedures ↴	CMA_C1299 - Review and update identification and authentication policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review and update incident response policies and procedures ↴	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review and update information integrity policies and procedures ↴	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review and update media protection policies and procedures ↴	CMA_C1427 - Review and update media protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review and update personnel security policies and procedures ↴	CMA_C1507 - Review and update personnel security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review and update physical and environmental policies and procedures ↴	CMA_C1446 - Review and update physical and environmental policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review and update planning policies and procedures ↴	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review and update risk assessment policies and procedures ↴	CMA_C1537 - Review and update risk assessment policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review and update system and communications protection policies and procedures ↴	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review and update system and services acquisition policies and procedures ↴	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review and update system maintenance policies and procedures ↴	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review security assessment and authorization policies and procedures ↴	CMA_C1143 - Review security assessment and authorization policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Update information security	CMA_0518 - Update information	Manual,	<a href="#">1.1.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
policies ↗	security policies	Disabled	
Update privacy plan, policies, and procedures ↗	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	1.1.0 ↗

## Intellectual property rights

ID: ISO 27001:2013 A.18.1.2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require compliance with intellectual property rights ↗	CMA_0432 - Require compliance with intellectual property rights	Manual, Disabled	1.1.0 ↗
Track software license usage ↗	CMA_C1235 - Track software license usage	Manual, Disabled	1.1.0 ↗

## Protection of records

ID: ISO 27001:2013 A.18.1.3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize access to security functions and information ↗	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	1.1.0 ↗
Authorize and manage access ↗	CMA_0023 - Authorize and manage access	Manual, Disabled	1.1.0 ↗
Conduct backup of information system documentation ↗	CMA_C1289 - Conduct backup of information system documentation	Manual, Disabled	1.1.0 ↗
Control physical access ↗	CMA_0081 - Control physical access	Manual, Disabled	1.1.0 ↗
Enable dual or joint authorization ↗	CMA_0226 - Enable dual or joint authorization	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce logical access ↗	CMA_0245 - Enforce logical access	Manual, Disabled	1.1.0 ↗
Ensure information system fails in known state ↗	CMA_C1662 - Ensure information system fails in known state	Manual, Disabled	1.1.0 ↗
Establish backup policies and procedures ↗	CMA_0268 - Establish backup policies and procedures	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Implement transaction based recovery ↗	CMA_C1296 - Implement transaction based recovery	Manual, Disabled	1.1.0 ↗
Manage the input, output, processing, and storage of data ↗	CMA_0369 - Manage the input, output, processing, and storage of data	Manual, Disabled	1.1.0 ↗
Protect audit information ↗	CMA_0401 - Protect audit information	Manual, Disabled	1.1.0 ↗
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	1.1.0 ↗
Review label activity and analytics ↗	CMA_0474 - Review label activity and analytics	Manual, Disabled	1.1.0 ↗
Review user groups and applications with access to sensitive data ↗	CMA_0481 - Review user groups and applications with access to sensitive data	Manual, Disabled	1.1.0 ↗

## Privacy and protection of personally identifiable information

ID: ISO 27001:2013 A.18.1.4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Control physical access ↗	CMA_0081 - Control physical access	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	1.1.0 ↗
Manage compliance activities ↗	CMA_0358 - Manage compliance activities	Manual, Disabled	1.1.0 ↗
Manage the input, output, processing, and storage of data ↗	CMA_0369 - Manage the input, output, processing, and storage of data	Manual, Disabled	1.1.0 ↗
Review label activity and analytics ↗	CMA_0474 - Review label activity and analytics	Manual, Disabled	1.1.0 ↗

## Regulation of cryptographic controls

ID: ISO 27001:2013 A.18.1.5 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authenticate to cryptographic module ↗	CMA_0021 - Authenticate to cryptographic module	Manual, Disabled	1.1.0 ↗
Define cryptographic use ↗	CMA_0120 - Define cryptographic use	Manual, Disabled	1.1.0 ↗

## Independent review of information security

ID: ISO 27001:2013 A.18.2.1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ independent team for penetration testing ↗	CMA_C1171 - Employ independent team for penetration testing	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗

## Compliance with security policies and standards

ID: ISO 27001:2013 A.18.2.2 Ownership: Shared

  Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess Security Controls ↗	CMA_C1145 - Assess Security Controls	Manual, Disabled	1.1.0 ↗
Check for privacy and security compliance before establishing internal connections ↗	CMA_0053 - Check for privacy and security compliance before establishing internal connections	Manual, Disabled	1.1.0 ↗
Configure detection whitelist ↗	CMA_0068 - Configure detection whitelist	Manual, Disabled	1.1.0 ↗
Deliver security assessment results ↗	CMA_C1147 - Deliver security assessment results	Manual, Disabled	1.1.0 ↗
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	1.1.0 ↗
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	1.1.0 ↗
Develop audit and accountability policies and procedures ↗	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	1.1.0 ↗
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	1.1.0 ↗
Develop security assessment plan ↗	CMA_C1144 - Develop security assessment plan	Manual, Disabled	1.1.0 ↗
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	1.1.0 ↗
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗
Produce Security Assessment report ↗	CMA_C1146 - Produce Security Assessment report	Manual, Disabled	1.1.0 ↗
Protect the information security program plan ↗	CMA_C1732 - Protect the information security program plan	Manual, Disabled	1.1.0 ↗
Review access control policies and procedures ↗	CMA_0457 - Review access control policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update configuration management policies and procedures ↗	CMA_C1175 - Review and update configuration management policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update contingency planning policies and procedures ↗	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update identification and authentication policies and procedures ↗	CMA_C1299 - Review and update identification and authentication policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update incident response policies and procedures ↗	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update information integrity policies and procedures ↗	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update media protection policies and procedures ↗	CMA_C1427 - Review and update media protection policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update personnel security policies and procedures ↗	CMA_C1507 - Review and update personnel security policies and	Manual, Disabled	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal) <a href="#">Review and update physical and environmental policies and procedures ↗</a>	CMA_C1446 - Review and update physical and environmental policies and procedures	Manual, Disabled	(GitHub) <a href="#">1.1.0 ↗</a>
<a href="#">Review and update planning policies and procedures ↗</a>	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update risk assessment policies and procedures ↗</a>	CMA_C1537 - Review and update risk assessment policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update system and communications protection policies and procedures ↗</a>	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update system and services acquisition policies and procedures ↗</a>	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update system maintenance policies and procedures ↗</a>	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review security assessment and authorization policies and procedures ↗</a>	CMA_C1143 - Review security assessment and authorization policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Turn on sensors for endpoint security solution ↗</a>	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Undergo independent security review ↗</a>	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update information security policies ↗</a>	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update privacy plan, policies, and procedures ↗</a>	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Technical compliance review

ID: ISO 27001:2013 A.18.2.3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess Security Controls ↗</a>	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Deliver security assessment results ↗</a>	CMA_C1147 - Deliver security assessment results	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop security assessment plan ↗</a>	CMA_C1144 - Develop security assessment plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ independent team for penetration testing ↗</a>	CMA_C1171 - Employ independent team for penetration testing	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Produce Security Assessment report ↗</a>	CMA_C1146 - Produce Security Assessment report	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Information Security Policies

## Policies for information security

ID: ISO 27001:2013 A.5.1.1 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Determine supplier contract obligations ↗</a>	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop access control policies and procedures ↗</a>	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop and establish a system security plan ↗</a>	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop audit and accountability policies and procedures ↗</a>	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop information security policies and procedures ↗</a>	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document acquisition contract acceptance criteria ↗</a>	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document protection of personal data in acquisition contracts ↗	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document protection of security information in acquisition contracts ↗	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document requirements for the use of shared data in contracts ↗	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	1.1.0 ↗
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗
Document security assurance requirements in acquisition contracts ↗	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document security documentation requirements in acquisition contract ↗	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	1.1.0 ↗
Document security functional requirements in acquisition contracts ↗	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the protection of cardholder data in third party contracts ↗	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	1.1.0 ↗
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	1.1.0 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish privacy requirements for contractors and service providers ↗	CMA_C1810 - Establish privacy requirements for contractors and service providers	Manual, Disabled	1.1.0 ↗
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗
Manage compliance activities ↗	CMA_0358 - Manage compliance activities	Manual, Disabled	1.1.0 ↗
Protect the information security program plan ↗	CMA_C1732 - Protect the information security program plan	Manual, Disabled	1.1.0 ↗
Review access control policies and procedures ↗	CMA_0457 - Review access control policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update configuration management policies and procedures ↗	CMA_C1175 - Review and update configuration management policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update contingency planning policies and procedures ↗	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update identification and authentication policies and procedures ↗	CMA_C1299 - Review and update identification and authentication policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update incident response policies and procedures ↗	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update information integrity policies and procedures ↗	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update media protection policies and procedures ↗	CMA_C1427 - Review and update media protection policies and procedures	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update personnel security policies and procedures ↗	CMA_C1507 - Review and update personnel security policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update physical and environmental policies and procedures ↗	CMA_C1446 - Review and update physical and environmental policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update planning policies and procedures ↗	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update risk assessment policies and procedures ↗	CMA_C1537 - Review and update risk assessment policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update system and communications protection policies and procedures ↗	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update system and services acquisition policies and procedures ↗	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update system maintenance policies and procedures ↗	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	1.1.0 ↗
Review security assessment and authorization policies and procedures ↗	CMA_C1143 - Review security assessment and authorization policies and procedures	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗
Update privacy plan, policies, and procedures ↗	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	1.1.0 ↗

## Review of the policies for information security

ID: ISO 27001:2013 A.5.1.2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop audit and accountability policies and procedures ↗	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect the information security program plan ↗	CMA_C1732 - Protect the information security program plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review access control policies and procedures ↗	CMA_0457 - Review access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update configuration management policies and procedures ↗	CMA_C1175 - Review and update configuration management policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update contingency planning policies and procedures ↗	CMA_C1243 - Review and update contingency planning policies and	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
<a href="#">(Azure portal) Review and update identification and authentication policies and procedures ↴</a>	CMA_C1299 - Review and update identification and authentication policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Review and update incident response policies and procedures ↴</a>	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Review and update information integrity policies and procedures ↴</a>	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Review and update media protection policies and procedures ↴</a>	CMA_C1427 - Review and update media protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Review and update personnel security policies and procedures ↴</a>	CMA_C1507 - Review and update personnel security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Review and update physical and environmental policies and procedures ↴</a>	CMA_C1446 - Review and update physical and environmental policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Review and update planning policies and procedures ↴</a>	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Review and update risk assessment policies and procedures ↴</a>	CMA_C1537 - Review and update risk assessment policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Review and update system and communications protection policies and procedures ↴</a>	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Review and update system and services acquisition policies and procedures ↴</a>	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Review and update system maintenance policies and procedures ↴</a>	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Review security assessment and authorization policies and procedures ↴</a>	CMA_C1143 - Review security assessment and authorization policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Update information security policies ↴</a>	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Update privacy plan, policies, and procedures ↗	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Organization of Information Security

## Information security roles and responsibilities

ID: ISO 27001:2013 A.6.1.1 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Appoint a senior information security officer ↗	CMA_C1733 - Appoint a senior information security officer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Communicate contingency plan changes ↗	CMA_C1249 - Communicate contingency plan changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Create configuration plan protection ↗	CMA_C1233 - Create configuration plan protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Define and document government oversight ↗	CMA_C1587 - Define and document government oversight	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Define information security roles and responsibilities ↗	CMA_C1565 - Define information security roles and responsibilities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Designate individuals to fulfill specific roles and responsibilities ↗	CMA_C1747 - Designate individuals to fulfill specific roles and responsibilities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Determine supplier contract obligations ↗	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and document a business continuity and disaster recovery plan ↗	CMA_0146 - Develop and document a business continuity and disaster recovery plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and maintain baseline configurations ↗	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop audit and accountability policies and procedures ↗	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop configuration item identification plan ↗	CMA_C1231 - Develop configuration item identification plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop configuration management plan ↗	CMA_C1232 - Develop configuration management plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop contingency planning policies and procedures ↗	CMA_0156 - Develop contingency planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Distribute policies and procedures ↗	CMA_0185 - Distribute policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document acquisition contract acceptance criteria ↗	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document and implement privacy complaint procedures ↗	CMA_0189 - Document and implement privacy complaint procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document protection of personal data in acquisition contracts ↗	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document protection of security information in acquisition contracts ↗	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document requirements for the use of shared data in contracts ↗	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security and privacy	CMA_0198 - Document security and	Manual,	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">training activities ↗</a>	privacy training activities	Disabled	
<a href="#">Document security assurance requirements in acquisition contracts ↗</a>	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security documentation requirements in acquisition contract ↗</a>	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security functional requirements in acquisition contracts ↗</a>	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security strength requirements in acquisition contracts ↗</a>	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document the information system environment in acquisition contracts ↗</a>	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document the protection of cardholder data in third party contracts ↗</a>	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document third-party personnel security requirements ↗</a>	CMA_C1531 - Document third-party personnel security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce mandatory and discretionary access control policies ↗</a>	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Ensure privacy program information is publicly available ↗</a>	CMA_C1867 - Ensure privacy program information is publicly available	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a privacy program ↗</a>	CMA_0257 - Establish a privacy program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish an information security program ↗</a>	CMA_0263 - Establish an information security program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and document a configuration management plan ↗</a>	CMA_0264 - Establish and document a configuration management plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish security requirements for the manufacturing of connected devices ↗</a>	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0 ↗
Identify individuals with security roles and responsibilities ↗	CMA_C1566 - Identify individuals with security roles and responsibilities	Manual, Disabled	1.1.1 ↗
Implement an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	1.1.0 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗
Integrate risk management process into SDLC ↗	CMA_C1567 - Integrate risk management process into SDLC	Manual, Disabled	1.1.0 ↗
Manage security state of information systems ↗	CMA_C1746 - Manage security state of information systems	Manual, Disabled	1.1.0 ↗
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	Manual, Disabled	1.1.0 ↗
Plan for resumption of essential business functions ↗	CMA_C1253 - Plan for resumption of essential business functions	Manual, Disabled	1.1.0 ↗
Protect the information security program plan ↗	CMA_C1732 - Protect the information security program plan	Manual, Disabled	1.1.0 ↗
Require external service providers to comply with security requirements ↗	CMA_C1586 - Require external service providers to comply with security requirements	Manual, Disabled	1.1.0 ↗
Require notification of third-party personnel transfer or termination ↗	CMA_C1532 - Require notification of third-party personnel transfer or termination	Manual, Disabled	1.1.0 ↗
Require third-party providers to comply with personnel security policies and procedures ↗	CMA_C1530 - Require third-party providers to comply with personnel security policies and procedures	Manual, Disabled	1.1.0 ↗
Resume all mission and business functions ↗	CMA_C1254 - Resume all mission and business functions	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review access control policies and procedures ↗</a>	CMA_0457 - Review access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update configuration management policies and procedures ↗</a>	CMA_C1175 - Review and update configuration management policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update contingency planning policies and procedures ↗</a>	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update identification and authentication policies and procedures ↗</a>	CMA_C1299 - Review and update identification and authentication policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update incident response policies and procedures ↗</a>	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update information integrity policies and procedures ↗</a>	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update media protection policies and procedures ↗</a>	CMA_C1427 - Review and update media protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update personnel security policies and procedures ↗</a>	CMA_C1507 - Review and update personnel security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update physical and environmental policies and procedures ↗</a>	CMA_C1446 - Review and update physical and environmental policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update planning policies and procedures ↗</a>	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update risk assessment policies and procedures ↗</a>	CMA_C1537 - Review and update risk assessment policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update system and communications protection policies and procedures ↗</a>	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update system and services acquisition policies and</a>	CMA_C1560 - Review and update system and services acquisition	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
procedures ↗	policies and procedures		
Review and update system maintenance policies and procedures ↗	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	1.1.0 ↗
Review cloud service provider's compliance with policies and agreements ↗	CMA_0469 - Review cloud service provider's compliance with policies and agreements	Manual, Disabled	1.1.0 ↗
Review contingency plan ↗	CMA_C1247 - Review contingency plan	Manual, Disabled	1.1.0 ↗
Review security assessment and authorization policies and procedures ↗	CMA_C1143 - Review security assessment and authorization policies and procedures	Manual, Disabled	1.1.0 ↗
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	1.1.0 ↗
Update contingency plan ↗	CMA_C1248 - Update contingency plan	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗
Update privacy plan, policies, and procedures ↗	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	1.1.0 ↗

## Segregation of Duties

ID: ISO 27001:2013 A.6.1.2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
A maximum of 3 owners should be designated for your subscription ↗	It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.	AuditIfNotExists, Disabled	3.0.0 ↗
Define access authorizations to support separation of duties ↗	CMA_0116 - Define access authorizations to support separation of duties	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document separation of duties ↗	CMA_0204 - Document separation of duties	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Separate duties of individuals ↗	CMA_0492 - Separate duties of individuals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
There should be more than one owner assigned to your subscription ↗	It is recommended to designate more than one subscription owner in order to have administrator access redundancy.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Contact with authorities

ID: ISO 27001:2013 A.6.1.3 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage contacts for authorities and special interest groups ↗	CMA_0359 - Manage contacts for authorities and special interest groups	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Contact with special interest groups

ID: ISO 27001:2013 A.6.1.4 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Disseminate security alerts to personnel ↗	CMA_C1705 - Disseminate security alerts to personnel	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a threat intelligence	CMA_0260 - Establish a threat	Manual,	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
program ↗	intelligence program	Disabled	
Generate internal security alerts ↗	CMA_C1704 - Generate internal security alerts	Manual, Disabled	1.1.0 ↗
Implement security directives ↗	CMA_C1706 - Implement security directives	Manual, Disabled	1.1.0 ↗
Manage contacts for authorities and special interest groups ↗	CMA_0359 - Manage contacts for authorities and special interest groups	Manual, Disabled	1.1.0 ↗

## Information security in project management

ID: ISO 27001:2013 A.6.1.5 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Align business objectives and IT goals ↗	CMA_0008 - Align business objectives and IT goals	Manual, Disabled	1.1.0 ↗
Allocate resources in determining information system requirements ↗	CMA_C1561 - Allocate resources in determining information system requirements	Manual, Disabled	1.1.0 ↗
Define and document government oversight ↗	CMA_C1587 - Define and document government oversight	Manual, Disabled	1.1.0 ↗
Define information security roles and responsibilities ↗	CMA_C1565 - Define information security roles and responsibilities	Manual, Disabled	1.1.0 ↗
Determine supplier contract obligations ↗	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	1.1.0 ↗
Document acquisition contract acceptance criteria ↗	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	1.1.0 ↗
Document protection of personal data in acquisition contracts ↗	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document protection of security information in acquisition	CMA_0195 - Document protection of security information in	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">contracts ↗</a>	acquisition contracts		
<a href="#">Document requirements for the use of shared data in contracts ↗</a>	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security assurance requirements in acquisition contracts ↗</a>	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security documentation requirements in acquisition contract ↗</a>	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security functional requirements in acquisition contracts ↗</a>	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security strength requirements in acquisition contracts ↗</a>	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document the information system environment in acquisition contracts ↗</a>	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document the protection of cardholder data in third party contracts ↗</a>	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a discrete line item in budgeting documentation ↗</a>	CMA_C1563 - Establish a discrete line item in budgeting documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a privacy program ↗</a>	CMA_0257 - Establish a privacy program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Govern the allocation of resources ↗</a>	CMA_0293 - Govern the allocation of resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify individuals with security roles and responsibilities ↗</a>	CMA_C1566 - Identify individuals with security roles and responsibilities	Manual, Disabled	<a href="#">1.1.1 ↗</a>
<a href="#">Integrate risk management process into SDLC ↗</a>	CMA_C1567 - Integrate risk management process into SDLC	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require external service providers to comply with security</a>	CMA_C1586 - Require external service providers to comply with	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
requirements ↗	security requirements		
Review cloud service provider's compliance with policies and agreements ↗	CMA_0469 - Review cloud service provider's compliance with policies and agreements	Manual, Disabled	1.1.0 ↗
Review development process, standards and tools ↗	CMA_C1610 - Review development process, standards and tools	Manual, Disabled	1.1.0 ↗
Secure commitment from leadership ↗	CMA_0489 - Secure commitment from leadership	Manual, Disabled	1.1.0 ↗
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	1.1.0 ↗

## Mobile device policy

ID: ISO 27001:2013 A.6.2.1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adopt biometric authentication mechanisms ↗	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	1.1.0 ↗
Authorize remote access ↗	CMA_0024 - Authorize remote access	Manual, Disabled	1.1.0 ↗
Define mobile device requirements ↗	CMA_0122 - Define mobile device requirements	Manual, Disabled	1.1.0 ↗
Document and implement wireless access guidelines ↗	CMA_0190 - Document and implement wireless access guidelines	Manual, Disabled	1.1.0 ↗
Document mobility training ↗	CMA_0191 - Document mobility training	Manual, Disabled	1.1.0 ↗
Document remote access guidelines ↗	CMA_0196 - Document remote access guidelines	Manual, Disabled	1.1.0 ↗
Identify and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure alternate work sites ↗	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	1.1.0 ↗
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	1.1.0 ↗
Notify users of system logon or access ↗	CMA_0382 - Notify users of system logon or access	Manual, Disabled	1.1.0 ↗
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗
Protect wireless access ↗	CMA_0411 - Protect wireless access	Manual, Disabled	1.1.0 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗

## Teleworking

ID: ISO 27001:2013 A.6.2.2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adopt biometric authentication mechanisms ↗	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	1.1.0 ↗
Authorize access to security functions and information ↗	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	1.1.0 ↗
Authorize and manage access ↗	CMA_0023 - Authorize and manage access	Manual, Disabled	1.1.0 ↗
Authorize remote access ↗	CMA_0024 - Authorize remote access	Manual, Disabled	1.1.0 ↗
Document mobility training ↗	CMA_0191 - Document mobility training	Manual, Disabled	1.1.0 ↗
Document remote access guidelines ↗	CMA_0196 - Document remote access guidelines	Manual, Disabled	1.1.0 ↗
Enforce logical access ↗	CMA_0245 - Enforce logical access	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
		Disabled	
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	1.1.0 ↗
Identify and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	1.1.0 ↗
Implement controls to secure alternate work sites ↗	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	1.1.0 ↗
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	1.1.0 ↗
Notify users of system logon or access ↗	CMA_0382 - Notify users of system logon or access	Manual, Disabled	1.1.0 ↗
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	1.1.0 ↗
Review user groups and applications with access to sensitive data ↗	CMA_0481 - Review user groups and applications with access to sensitive data	Manual, Disabled	1.1.0 ↗

## Human Resources Security

### Screening

ID: ISO 27001:2013 A.7.1.1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Clear personnel with access to classified information ↗	CMA_0054 - Clear personnel with access to classified information	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement personnel screening ↗	CMA_0322 - Implement personnel screening	Manual, Disabled	1.1.0 ↗
Rescreen individuals at a defined frequency ↗	CMA_C1512 - Rescreen individuals at a defined frequency	Manual, Disabled	1.1.0 ↗

## Terms and conditions of employment

ID: ISO 27001:2013 A.7.1.2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Determine supplier contract obligations ↗	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	1.1.0 ↗
Develop acceptable use policies and procedures ↗	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	1.1.0 ↗
Develop security safeguards ↗	CMA_0161 - Develop security safeguards	Manual, Disabled	1.1.0 ↗
Document acquisition contract acceptance criteria ↗	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	1.1.0 ↗
Document organizational access agreements ↗	CMA_0192 - Document organizational access agreements	Manual, Disabled	1.1.0 ↗
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	Manual, Disabled	1.1.0 ↗
Document protection of personal data in acquisition contracts ↗	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document protection of security information in acquisition contracts ↗	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document requirements for the use of shared data in contracts ↗	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security assurance requirements in acquisition contracts ↗	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document security documentation requirements in acquisition contract ↗	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	1.1.0 ↗
Document security functional requirements in acquisition contracts ↗	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the protection of cardholder data in third party contracts ↗	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	1.1.0 ↗
Enforce rules of behavior and access agreements ↗	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Ensure access agreements are signed or resigned timely ↗	CMA_C1528 - Ensure access agreements are signed or resigned timely	Manual, Disabled	1.1.0 ↗
Ensure privacy program information is publicly available ↗	CMA_C1867 - Ensure privacy program information is publicly available	Manual, Disabled	1.1.0 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗
Implement privacy notice delivery methods ↗	CMA_0324 - Implement privacy notice delivery methods	Manual, Disabled	1.1.0 ↗
Obtain consent prior to collection or processing of personal data ↗	CMA_0385 - Obtain consent prior to collection or processing of personal data	Manual, Disabled	1.1.0 ↗
Provide privacy notice ↗	CMA_0414 - Provide privacy notice	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require users to sign access agreement ↗	CMA_0440 - Require users to sign access agreement	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update organizational access agreements ↗	CMA_0520 - Update organizational access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Management responsibilities

ID: ISO 27001:2013 A.7.2.1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define and document government oversight ↗	CMA_C1587 - Define and document government oversight	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Determine supplier contract obligations ↗	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop acceptable use policies and procedures ↗	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document acquisition contract acceptance criteria ↗	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document organizational access agreements ↗	CMA_0192 - Document organizational access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document protection of personal data in acquisition contracts ↗	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document protection of security information in acquisition contracts ↗	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document requirements for the use of shared data in contracts ↗	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security assurance requirements in acquisition contracts ↗	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security documentation requirements in acquisition contract ↗	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security functional requirements in acquisition contracts ↗	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document the protection of cardholder data in third party contracts ↗	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document third-party personnel security requirements ↗	CMA_C1531 - Document third-party personnel security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce rules of behavior and access agreements ↗	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Ensure access agreements are signed or resigned timely ↗	CMA_C1528 - Ensure access agreements are signed or resigned timely	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require external service providers to comply with security requirements ↗	CMA_C1586 - Require external service providers to comply with security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require notification of third-party personnel transfer or termination ↗	CMA_C1532 - Require notification of third-party personnel transfer or termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require third-party providers to comply with personnel security policies and procedures ↗	CMA_C1530 - Require third-party providers to comply with personnel security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require users to sign access agreement ↗	CMA_0440 - Require users to sign access agreement	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review cloud service provider's compliance with policies and agreements ↗	CMA_0469 - Review cloud service provider's compliance with policies and agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update organizational access agreements ↗	CMA_0520 - Update organizational access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information security awareness, education and training

ID: ISO 27001:2013 A.7.2.2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Employ automated training environment ↗	CMA_C1357 - Employ automated training environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish information security workforce development and improvement program ↗	CMA_C1752 - Establish information security workforce development and improvement program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor security and privacy training completion ↗	CMA_0379 - Monitor security and privacy training completion	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Provide contingency training ↗	CMA_0412 - Provide contingency training	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Provide periodic role-based security training ↗	CMA_C1095 - Provide periodic role-based security training	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Provide periodic security awareness training ↗	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗
Provide role-based security training ↗	CMA_C1094 - Provide role-based security training	Manual, Disabled	1.1.0 ↗
Provide security training before providing access ↗	CMA_0418 - Provide security training before providing access	Manual, Disabled	1.1.0 ↗
Provide security training for new users ↗	CMA_0419 - Provide security training for new users	Manual, Disabled	1.1.0 ↗
Provide updated security awareness training ↗	CMA_C1090 - Provide updated security awareness training	Manual, Disabled	1.1.0 ↗
Retain training records ↗	CMA_0456 - Retain training records	Manual, Disabled	1.1.0 ↗
Train personnel on disclosure of nonpublic information ↗	CMA_C1084 - Train personnel on disclosure of nonpublic information	Manual, Disabled	1.1.0 ↗

## Disciplinary process

ID: ISO 27001:2013 A.7.2.3 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement formal sanctions process ↗	CMA_0317 - Implement formal sanctions process	Manual, Disabled	1.1.0 ↗
Notify personnel upon sanctions ↗	CMA_0380 - Notify personnel upon sanctions	Manual, Disabled	1.1.0 ↗

## Termination or change of employment responsibilities

ID: ISO 27001:2013 A.7.3.1 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct exit interview upon termination ↗	CMA_0058 - Conduct exit interview upon termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Initiate transfer or reassignment actions ↗	CMA_0333 - Initiate transfer or reassignment actions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Modify access authorizations upon personnel transfer ↗	CMA_0374 - Modify access authorizations upon personnel transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify upon termination or transfer ↗	CMA_0381 - Notify upon termination or transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect against and prevent data theft from departing employees ↗	CMA_0398 - Protect against and prevent data theft from departing employees	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Reevaluate access upon personnel transfer ↗	CMA_0424 - Reevaluate access upon personnel transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Asset Management

### Inventory of assets

ID: ISO 27001:2013 A.8.1.1 Ownership: Shared

[] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Create a data inventory ↗	CMA_0096 - Create a data inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Maintain records of processing of personal data ↗	CMA_0353 - Maintain records of processing of personal data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Ownership of assets

ID: ISO 27001:2013 A.8.1.2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↗
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	Manual, Disabled	1.1.0 ↗
Create a data inventory ↗	CMA_0096 - Create a data inventory	Manual, Disabled	1.1.0 ↗
Establish and maintain an asset inventory ↗	CMA_0266 - Establish and maintain an asset inventory	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Maintain records of processing of personal data ↗	CMA_0353 - Maintain records of processing of personal data	Manual, Disabled	1.1.0 ↗
Restrict media use ↗	CMA_0450 - Restrict media use	Manual, Disabled	1.1.0 ↗

## Acceptable use of assets

ID: ISO 27001:2013 A.8.1.3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop acceptable use policies and procedures ↗	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	1.1.0 ↗
Enforce rules of behavior and access agreements ↗	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗

## Return of assets

ID: ISO 27001:2013 A.8.1.4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct exit interview upon termination ↗	CMA_0058 - Conduct exit interview upon termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Initiate transfer or reassignment actions ↗	CMA_0333 - Initiate transfer or reassignment actions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Modify access authorizations upon personnel transfer ↗	CMA_0374 - Modify access authorizations upon personnel transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify upon termination or transfer ↗	CMA_0381 - Notify upon termination or transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect against and prevent data theft from departing employees ↗	CMA_0398 - Protect against and prevent data theft from departing employees	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Reevaluate access upon personnel transfer ↗	CMA_0424 - Reevaluate access upon personnel transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Classification of information

ID: ISO 27001:2013 A.8.2.1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Categorize information ↗	CMA_0052 - Categorize information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop business classification schemes ↗	CMA_0155 - Develop business classification schemes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Ensure security categorization is	CMA_C1540 - Ensure security categorization is approved	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
approved ↗			
Review label activity and analytics ↗	CMA_0474 - Review label activity and analytics	Manual, Disabled	1.1.0 ↗
SQL databases should have vulnerability findings resolved ↗	Monitor vulnerability assessment scan results and recommendations for how to remediate database vulnerabilities.	AuditIfNotExists, Disabled	4.1.0 ↗

## Labelling of information

ID: ISO 27001:2013 A.8.2.2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Control physical access ↗	CMA_0081 - Control physical access	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Manage the input, output, processing, and storage of data ↗	CMA_0369 - Manage the input, output, processing, and storage of data	Manual, Disabled	1.1.0 ↗
Review label activity and analytics ↗	CMA_0474 - Review label activity and analytics	Manual, Disabled	1.1.0 ↗

## Handling of assets

ID: ISO 27001:2013 A.8.2.3 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure workstations to check for digital certificates ↗	CMA_0073 - Configure workstations to check for digital certificates	Manual, Disabled	1.1.0 ↗
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	1.1.0 ↗
Control physical access ↗	CMA_0081 - Control physical access	Manual, Disabled	1.1.0 ↗
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	Manual, Disabled	1.1.0 ↗
Define requirements for managing assets ↗	CMA_0125 - Define requirements for managing assets	Manual, Disabled	1.1.0 ↗
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Establish a data leakage management procedure ↗	CMA_0255 - Establish a data leakage management procedure	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗
Establish firewall and router configuration standards ↗	CMA_0272 - Establish firewall and router configuration standards	Manual, Disabled	1.1.0 ↗
Establish network segmentation for card holder data environment ↗	CMA_0273 - Establish network segmentation for card holder data environment	Manual, Disabled	1.1.0 ↗
Identify and manage downstream information exchanges ↗	CMA_0298 - Identify and manage downstream information exchanges	Manual, Disabled	1.1.0 ↗
Implement a fault tolerant name/address service ↗	CMA_0305 - Implement a fault tolerant name/address service	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Manage the input, output, processing, and storage of data ↗	CMA_0369 - Manage the input, output, processing, and storage of data	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗
Produce, control and distribute asymmetric cryptographic keys ↗	CMA_C1646 - Produce, control and distribute asymmetric cryptographic keys	Manual, Disabled	1.1.0 ↗
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	1.1.0 ↗
Protect special information ↗	CMA_0409 - Protect special information	Manual, Disabled	1.1.0 ↗
Provide secure name and address resolution services ↗	CMA_0416 - Provide secure name and address resolution services	Manual, Disabled	1.1.0 ↗
Restrict media use ↗	CMA_0450 - Restrict media use	Manual, Disabled	1.1.0 ↗
Review label activity and analytics ↗	CMA_0474 - Review label activity and analytics	Manual, Disabled	1.1.0 ↗

## Management of removable media

ID: ISO 27001:2013 A.8.3.1 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	Manual, Disabled	1.1.0 ↗
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗
Restrict media use ↗	CMA_0450 - Restrict media use	Manual, Disabled	1.1.0 ↗

## Disposal of media

ID: ISO 27001:2013 A.8.3.2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗

## Physical media transfer

ID: ISO 27001:2013 A.8.3.3 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗

# Access Control

## Access control policy

ID: ISO 27001:2013 A.9.1.1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop access control policies and procedures ↗</a>	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce mandatory and discretionary access control policies ↗</a>	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Govern policies and procedures ↗</a>	CMA_0292 - Govern policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review access control policies and procedures ↗</a>	CMA_0457 - Review access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Access to networks and network services

ID: ISO 27001:2013 A.9.1.2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	modify	<a href="#">1.2.0 ↗</a>
<a href="#">Add system-assigned managed</a>	This policy adds a system-assigned managed identity to virtual machines	modify	<a href="#">1.2.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↴</a>	hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴.		
<a href="#">Adopt biometric authentication mechanisms ↴</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Audit Linux machines that allow remote connections from accounts without passwords ↴</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴. Machines are non-compliant if Linux machines that allow remote connections from accounts without passwords	AuditIfNotExists, Disabled	<a href="#">1.3.0 ↴</a>
<a href="#">Audit Linux machines that have accounts without passwords ↴</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴. Machines are non-compliant if Linux machines that have accounts without passwords	AuditIfNotExists, Disabled	<a href="#">1.3.0 ↴</a>
<a href="#">Audit VMs that do not use managed disks ↴</a>	This policy audits VMs that do not use managed disks	audit	<a href="#">1.0.0 ↴</a>
<a href="#">Authorize access to security functions and information ↴</a>	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Authorize and manage access ↴</a>	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Automate account management ↴</a>	CMA_0026 - Automate account management	Manual, Disabled	<a href="#">1.1.0 ↴</a>
<a href="#">Deploy the Linux Guest Configuration extension to enable Guest Configuration</a>	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a	deployIfNotExists	<a href="#">1.3.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
assignments on Linux VMs ↗	prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .		
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	<a href="#">1.1.0</a> ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege access	Manual, Disabled	<a href="#">1.1.0</a> ↗
Enable detection of network devices ↗	CMA_0220 - Enable detection of network devices	Manual, Disabled	<a href="#">1.1.0</a> ↗
Enforce logical access ↗	CMA_0245 - Enforce logical access	Manual, Disabled	<a href="#">1.1.0</a> ↗
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0</a> ↗
Enforce user uniqueness ↗	CMA_0250 - Enforce user uniqueness	Manual, Disabled	<a href="#">1.1.0</a> ↗
Establish electronic signature and certificate requirements ↗	CMA_0271 - Establish electronic signature and certificate requirements	Manual, Disabled	<a href="#">1.1.0</a> ↗
Identify actions allowed without authentication ↗	CMA_0295 - Identify actions allowed without authentication	Manual, Disabled	<a href="#">1.1.0</a> ↗
Identify and authenticate non-organizational users ↗	CMA_C1346 - Identify and authenticate non-organizational users	Manual, Disabled	<a href="#">1.1.0</a> ↗
Manage system and admin accounts ↗	CMA_0368 - Manage system and admin accounts	Manual, Disabled	<a href="#">1.1.0</a> ↗
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	<a href="#">1.1.0</a> ↗
Notify when account is not needed ↗	CMA_0383 - Notify when account is not needed	Manual, Disabled	<a href="#">1.1.0</a> ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review user groups and applications with access to sensitive data ↗	CMA_0481 - Review user groups and applications with access to sensitive data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Set automated notifications for new and trending cloud applications in your organization ↗	CMA_0495 - Set automated notifications for new and trending cloud applications in your organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Storage accounts should be migrated to new Azure Resource Manager resources ↗	Use new Azure Resource Manager for your storage accounts to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
Support personal verification credentials issued by legal authorities ↗	CMA_0507 - Support personal verification credentials issued by legal authorities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Virtual machines should be migrated to new Azure Resource Manager resources ↗	Use new Azure Resource Manager for your virtual machines to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>

## User registration and de-registration

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assign account managers ↗</a>	CMA_0015 - Assign account managers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Assign system identifiers ↗</a>	CMA_0018 - Assign system identifiers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define information system account types ↗</a>	CMA_0121 - Define information system account types	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document access privileges ↗</a>	CMA_0186 - Document access privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enable detection of network devices ↗</a>	CMA_0220 - Enable detection of network devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce user uniqueness ↗</a>	CMA_0250 - Enforce user uniqueness	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish authenticator types and processes ↗</a>	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish conditions for role membership ↗</a>	CMA_0269 - Establish conditions for role membership	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish procedures for initial authenticator distribution ↗</a>	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify actions allowed without authentication ↗</a>	CMA_0295 - Identify actions allowed without authentication	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify and authenticate non-organizational users ↗</a>	CMA_C1346 - Identify and authenticate non-organizational users	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement training for protecting authenticators ↗</a>	CMA_0329 - Implement training for protecting authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage authenticator lifetime and reuse ↗</a>	CMA_0355 - Manage authenticator lifetime and reuse	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage Authenticators ↗</a>	CMA_C1321 - Manage	Manual,	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Authenticators	Disabled	
Notify Account Managers of customer controlled accounts ↗	CMA_C1009 - Notify Account Managers of customer controlled accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Prevent identifier reuse for the defined time period ↗	CMA_C1314 - Prevent identifier reuse for the defined time period	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Refresh authenticators ↗	CMA_0425 - Refresh authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Reissue authenticators for changed groups and accounts ↗	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review account provisioning logs ↗	CMA_0460 - Review account provisioning logs	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and reevaluate privileges ↗	CMA_C1207 - Review and reevaluate privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review user accounts ↗	CMA_0480 - Review user accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Set automated notifications for new and trending cloud applications in your organization ↗	CMA_0495 - Set automated notifications for new and trending cloud applications in your organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Support personal verification credentials issued by legal authorities ↗	CMA_0507 - Support personal verification credentials issued by legal authorities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## User access provisioning

ID: ISO 27001:2013 A.9.2.2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign account managers ↗	CMA_0015 - Assign account managers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Audit user account status ↗	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Authorize access to security functions and information ↗	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Authorize and manage access ↗	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Automate account management ↗	CMA_0026 - Automate account management	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Define information system account types ↗	CMA_0121 - Define information system account types	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document access privileges ↗	CMA_0186 - Document access privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish conditions for role membership ↗	CMA_0269 - Establish conditions for role membership	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Limit privileges to make changes in production environment ↗	CMA_C1206 - Limit privileges to make changes in production environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage system and admin accounts ↗	CMA_0368 - Manage system and admin accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify Account Managers of customer controlled accounts ↗	CMA_C1009 - Notify Account Managers of customer controlled accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify when account is not needed ↗	CMA_0383 - Notify when account is not needed	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review account provisioning logs ↗	CMA_0460 - Review account provisioning logs	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and reevaluate privileges ↗	CMA_C1207 - Review and reevaluate privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review user accounts ↗	CMA_0480 - Review user accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Management of privileged access rights

ID: ISO 27001:2013 A.9.2.3 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Accounts with owner permissions on Azure resources should be MFA enabled ↗	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
Accounts with write permissions on Azure resources should be MFA enabled ↗	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
An Azure Active Directory administrator should be provisioned for SQL servers ↗	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
Assign account managers ↗	CMA_0015 - Assign account managers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Audit privileged	CMA_0019 - Audit privileged functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<b>functions ↗</b>			
<a href="#">Audit usage of custom RBAC roles ↗</a>	Audit built-in roles such as 'Owner, Contributer, Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Authorize access to security functions and information ↗</a>	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Authorize and manage access ↗</a>	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate account management ↗</a>	CMA_0026 - Automate account management	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define information system account types ↗</a>	CMA_0121 - Define information system account types	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Design an access control model ↗</a>	CMA_0129 - Design an access control model	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document access privileges ↗</a>	CMA_0186 - Document access privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ least privilege access ↗</a>	CMA_0212 - Employ least privilege access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce mandatory and discretionary access control policies ↗</a>	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and document change control processes ↗</a>	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish conditions for role membership ↗</a>	CMA_0269 - Establish conditions for role membership	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Guest accounts with owner permissions on Azure resources should be removed ↗</a>	External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Guest accounts with write permissions on Azure resources should be removed ↗	External accounts with write privileges should be removed from your subscription in order to prevent unmonitored access.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
Limit privileges to make changes in production environment ↗	CMA_C1206 - Limit privileges to make changes in production environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage system and admin accounts ↗	CMA_0368 - Manage system and admin accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor privileged role assignment ↗	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify Account Managers of customer controlled accounts ↗	CMA_C1009 - Notify Account Managers of customer controlled accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify when account is not needed ↗	CMA_0383 - Notify when account is not needed	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review account provisioning logs ↗	CMA_0460 - Review account provisioning logs	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and reevaluate privileges ↗	CMA_C1207 - Review and reevaluate privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review user accounts ↗	CMA_0480 - Review user accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Service Fabric clusters should only use Azure Active Directory for client authentication ↗	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	<a href="#">1.1.0 ↗</a>
Use privileged identity	CMA_0533 - Use privileged identity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
management ↗	management		

## Management of secret authentication information of users

ID: ISO 27001:2013 A.9.2.4 Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Accounts with owner permissions on Azure resources should be MFA enabled ↗	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	1.0.0 ↗
Accounts with read permissions on Azure resources should be MFA enabled ↗	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	1.0.0 ↗
Accounts with write permissions on Azure resources should be MFA enabled ↗	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	1.0.0 ↗
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗ .	modify	1.2.0 ↗
Add system-assigned managed identity to enable Guest Configuration assignments on VMs	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A	modify	1.2.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">with a user-assigned identity ↗</a>	system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.		
<a href="#">Audit Linux machines that do not have the passwd file permissions set to 0644 ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Linux machines that do not have the passwd file permissions set to 0644	AuditIfNotExists, Disabled	<a href="#">1.3.0</a> ↗
<a href="#">Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↗</a>	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	deployIfNotExists	<a href="#">1.3.0</a> ↗
<a href="#">Disable authenticators upon termination ↗</a>	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	<a href="#">1.1.0</a> ↗
<a href="#">Document security strength requirements in acquisition contracts ↗</a>	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0</a> ↗
<a href="#">Establish a password policy ↗</a>	CMA_0256 - Establish a password policy	Manual, Disabled	<a href="#">1.1.0</a> ↗
<a href="#">Establish authenticator types and processes ↗</a>	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	<a href="#">1.1.0</a> ↗
<a href="#">Establish procedures for initial authenticator distribution ↗</a>	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	<a href="#">1.1.0</a> ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement parameters for memorized secret verifiers ↴	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Implement training for protecting authenticators ↴	CMA_0329 - Implement training for protecting authenticators	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Manage authenticator lifetime and reuse ↴	CMA_0355 - Manage authenticator lifetime and reuse	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Manage Authenticators ↴	CMA_C1321 - Manage Authenticators	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Protect passwords with encryption ↴	CMA_0408 - Protect passwords with encryption	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Refresh authenticators ↴	CMA_0425 - Refresh authenticators	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Reissue authenticators for changed groups and accounts ↴	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Revoke privileged roles as appropriate ↴	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Verify identity before distributing authenticators ↴	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Review of user access rights

ID: ISO 27001:2013 A.9.2.5 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign account managers ↴	CMA_0015 - Assign account managers	Manual, Disabled	<a href="#">1.1.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Blocked accounts with owner permissions on Azure resources should be removed ↗</a>	Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Blocked accounts with read and write permissions on Azure resources should be removed ↗</a>	Deprecated accounts should be removed from your subscriptions. Deprecated accounts are accounts that have been blocked from signing in.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Define information system account types ↗</a>	CMA_0121 - Define information system account types	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document access privileges ↗</a>	CMA_0186 - Document access privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish conditions for role membership ↗</a>	CMA_0269 - Establish conditions for role membership	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Guest accounts with owner permissions on Azure resources should be removed ↗</a>	External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Guest accounts with write permissions on Azure resources should be removed ↗</a>	External accounts with write privileges should be removed from your subscription in order to prevent unmonitored access.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Notify Account Managers of customer controlled accounts ↗</a>	CMA_C1009 - Notify Account Managers of customer controlled accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Reassign or remove user privileges as needed ↗</a>	CMA_C1040 - Reassign or remove user privileges as needed	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require approval for account creation ↗</a>	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Restrict access to privileged accounts ↗</a>	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review account</a>	CMA_0460 - Review account	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">provisioning logs ↗</a>	provisioning logs		
<a href="#">Review and reevaluate privileges ↗</a>	CMA_C1207 - Review and reevaluate privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review user accounts ↗</a>	CMA_0480 - Review user accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review user privileges ↗</a>	CMA_C1039 - Review user privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Removal or adjustment of access rights

ID: ISO 27001:2013 A.9.2.6 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assign account managers ↗</a>	CMA_0015 - Assign account managers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Blocked accounts with owner permissions on Azure resources should be removed ↗</a>	Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Blocked accounts with read and write permissions on Azure resources should be removed ↗</a>	Deprecated accounts should be removed from your subscriptions. Deprecated accounts are accounts that have been blocked from signing in.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Define information system account types ↗</a>	CMA_0121 - Define information system account types	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document access privileges ↗</a>	CMA_0186 - Document access privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish conditions for role membership ↗</a>	CMA_0269 - Establish conditions for role membership	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Initiate transfer or</a>	CMA_0333 - Initiate transfer or	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
reassignment actions ↗	reassignment actions		
Modify access authorizations upon personnel transfer ↗	CMA_0374 - Modify access authorizations upon personnel transfer	Manual, Disabled	1.1.0 ↗
Notify Account Managers of customer controlled accounts ↗	CMA_C1009 - Notify Account Managers of customer controlled accounts	Manual, Disabled	1.1.0 ↗
Notify upon termination or transfer ↗	CMA_0381 - Notify upon termination or transfer	Manual, Disabled	1.1.0 ↗
Reevaluate access upon personnel transfer ↗	CMA_0424 - Reevaluate access upon personnel transfer	Manual, Disabled	1.1.0 ↗
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	1.1.0 ↗
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	1.1.0 ↗
Review account provisioning logs ↗	CMA_0460 - Review account provisioning logs	Manual, Disabled	1.1.0 ↗
Review and reevaluate privileges ↗	CMA_C1207 - Review and reevaluate privileges	Manual, Disabled	1.1.0 ↗
Review user accounts ↗	CMA_0480 - Review user accounts	Manual, Disabled	1.1.0 ↗

## Use of secret authentication information

ID: ISO 27001:2013 A.9.3.1 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	1.1.0 ↗
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish a password policy ↗	CMA_0256 - Establish a password policy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish authenticator types and processes ↗	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish procedures for initial authenticator distribution ↗	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement parameters for memorized secret verifiers ↗	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement training for protecting authenticators ↗	CMA_0329 - Implement training for protecting authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage authenticator lifetime and reuse ↗	CMA_0355 - Manage authenticator lifetime and reuse	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage Authenticators ↗	CMA_C1321 - Manage Authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Refresh authenticators ↗	CMA_0425 - Refresh authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Reissue authenticators for changed groups and accounts ↗	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Terminate customer controlled account credentials ↗	CMA_C1022 - Terminate customer controlled account credentials	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information access restriction

ID: ISO 27001:2013 A.9.4.1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize access to security functions and information ↴	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Authorize and manage access ↴	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Automate account management ↴	CMA_0026 - Automate account management	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Enforce logical access ↴	CMA_0245 - Enforce logical access	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Enforce mandatory and discretionary access control policies ↴	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Limit privileges to make changes in production environment ↴	CMA_C1206 - Limit privileges to make changes in production environment	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Manage system and admin accounts ↴	CMA_0368 - Manage system and admin accounts	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Monitor access across the organization ↴	CMA_0376 - Monitor access across the organization	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Notify when account is not needed ↴	CMA_0383 - Notify when account is not needed	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Require approval for account creation ↴	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Review user groups and applications with access to sensitive data ↴	CMA_0481 - Review user groups and applications with access to sensitive data	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Secure log-on procedures

ID: ISO 27001:2013 A.9.4.2 Ownership: Shared

 [Expand table](#)

Name (Azure portal)	Description	Effect(s) (GitHub)	Version
<a href="#">Accounts with owner permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Accounts with read permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Accounts with write permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enable detection of network devices ↗</a>	CMA_0220 - Enable detection of network devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce a limit of consecutive failed login attempts ↗</a>	CMA_C1044 - Enforce a limit of consecutive failed login attempts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce user uniqueness ↗</a>	CMA_0250 - Enforce user uniqueness	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish electronic signature and certificate requirements ↗</a>	CMA_0271 - Establish electronic signature and certificate requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Generate error messages ↗</a>	CMA_C1724 - Generate error messages	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify actions allowed without authentication ↗</a>	CMA_0295 - Identify actions allowed without authentication	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify and authenticate non-organizational users ↗</a>	CMA_C1346 - Identify and authenticate non-organizational users	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Obscure feedback information during authentication process ↗</a>	CMA_C1344 - Obscure feedback information during authentication process	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Reveal error messages ↗	CMA_C1725 - Reveal error messages	Manual, Disabled	1.1.0 ↗
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	1.1.0 ↗
Set automated notifications for new and trending cloud applications in your organization ↗	CMA_0495 - Set automated notifications for new and trending cloud applications in your organization	Manual, Disabled	1.1.0 ↗
Support personal verification credentials issued by legal authorities ↗	CMA_0507 - Support personal verification credentials issued by legal authorities	Manual, Disabled	1.1.0 ↗
Terminate user session automatically ↗	CMA_C1054 - Terminate user session automatically	Manual, Disabled	1.1.0 ↗

## Password management system

ID: ISO 27001:2013 A.9.4.3 Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	1.2.0 ↗
Add system-assigned managed identity to enable Guest Configuration assignments on VMs	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A	modify	1.2.0 ↗

Name (Azure portal)	Description	Effect(s) (GitHub)	Version
<a href="#">with a user-assigned identity ↗</a>	system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .		
<a href="#">Audit Windows machines that allow re-use of the passwords after the specified number of unique passwords ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that allow re-use of the passwords after the specified number of unique passwords. Default value for unique passwords is 24	AuditIfNotExists, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Audit Windows machines that do not have the maximum password age set to specified number of days ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not have the maximum password age set to specified number of days. Default value for maximum password age is 70 days	AuditIfNotExists, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Audit Windows machines that do not have the minimum password age set to specified number of days ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not have the minimum password age set to specified number of days. Default value for minimum password age is 1 day	AuditIfNotExists, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Audit Windows machines that do not have the password complexity setting enabled ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not have the password complexity setting enabled	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Audit Windows machines that do not restrict the minimum password length to specified number of characters ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Windows machines that do not restrict the minimum password length to specified number of characters.	AuditIfNotExists, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Default value for minimum password length is 14 characters		
Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs ↗	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	deployIfNotExists	<a href="#">1.2.0 ↗</a>
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a password policy ↗	CMA_0256 - Establish a password policy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish authenticator types and processes ↗	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish procedures for initial authenticator distribution ↗	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement parameters for memorized secret verifiers ↗	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement training for protecting authenticators ↗	CMA_0329 - Implement training for protecting authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Manage authenticator lifetime and reuse ↗	CMA_0355 - Manage authenticator lifetime and reuse	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Manage Authenticators ↗	CMA_C1321 - Manage Authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Refresh authenticators ↗	CMA_0425 - Refresh authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Reissue authenticators for changed groups and accounts ↗	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Use of privileged utility programs

ID: ISO 27001:2013 A.9.4.4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize access to security functions and information ↗	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Authorize and manage access ↗	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Employ least privilege access ↗	CMA_0212 - Employ least privilege access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce logical access ↗	CMA_0245 - Enforce logical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review user groups and applications with access to sensitive data ↗	CMA_0481 - Review user groups and applications with access to sensitive data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Access control to program source code

ID: ISO 27001:2013 A.9.4.5 Ownership: Shared

[+] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize access to security functions and information ↗	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Authorize and manage access ↗	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Employ least privilege access ↗	CMA_0212 - Employ least privilege access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce logical access ↗	CMA_0245 - Enforce logical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Limit privileges to make changes in production environment ↗	CMA_C1206 - Limit privileges to make changes in production environment	Manual, Disabled	1.1.0 ↗
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	1.1.0 ↗
Review user groups and applications with access to sensitive data ↗	CMA_0481 - Review user groups and applications with access to sensitive data	Manual, Disabled	1.1.0 ↗

## Improvement

### Nonconformity and corrective action

ID: ISO 27001:2013 C.10.1.d Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Update POA&M items ↗	CMA_C1157 - Update POA&M items	Manual, Disabled	1.1.0 ↗

### Nonconformity and corrective action

ID: ISO 27001:2013 C.10.1.e Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Update POA&M items ↗	CMA_C1157 - Update POA&M items	Manual, Disabled	1.1.0 ↗

### Nonconformity and corrective action

ID: ISO 27001:2013 C.10.1.f Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update POA&M items ↗	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Nonconformity and corrective action

ID: ISO 27001:2013 C.10.1.g Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update POA&M items ↗	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Context of the organization

### Determining the scope of the information security management system

ID: ISO 27001:2013 C.4.3.a Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop SSP that meets criteria ↗	CMA_C1492 - Develop SSP that meets criteria	Manual, Disabled	1.1.0 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗

## Determining the scope of the information security management system

ID: ISO 27001:2013 C.4.3.b Ownership: Shared

↔ Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop SSP that meets criteria ↗	CMA_C1492 - Develop SSP that meets criteria	Manual, Disabled	1.1.0 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗

## Determining the scope of the information security management system

ID: ISO 27001:2013 C.4.3.c Ownership: Shared

↔ Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Align business objectives and IT goals ↗	CMA_0008 - Align business objectives and IT goals	Manual, Disabled	1.1.0 ↗
Determine supplier contract	CMA_0140 - Determine supplier	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">obligations ↗</a>	contract obligations	Disabled	
<a href="#">Develop SSP that meets criteria ↗</a>	CMA_C1492 - Develop SSP that meets criteria	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document acquisition contract acceptance criteria ↗</a>	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document protection of personal data in acquisition contracts ↗</a>	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document protection of security information in acquisition contracts ↗</a>	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document requirements for the use of shared data in contracts ↗</a>	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security assurance requirements in acquisition contracts ↗</a>	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security documentation requirements in acquisition contract ↗</a>	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security functional requirements in acquisition contracts ↗</a>	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security strength requirements in acquisition contracts ↗</a>	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document the information system environment in acquisition contracts ↗</a>	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document the protection of cardholder data in third party contracts ↗</a>	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ business case to record the resources required ↗</a>	CMA_C1735 - Employ business case to record the resources required	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Ensure capital planning and investment requests include necessary resources ↗</a>	CMA_C1734 - Ensure capital planning and investment requests include necessary resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish privacy requirements for contractors and service providers ↗	CMA_C1810 - Establish privacy requirements for contractors and service providers	Manual, Disabled	1.1.0 ↗
Govern the allocation of resources ↗	CMA_0293 - Govern the allocation of resources	Manual, Disabled	1.1.0 ↗
Secure commitment from leadership ↗	CMA_0489 - Secure commitment from leadership	Manual, Disabled	1.1.0 ↗

## Information security management system

ID: ISO 27001:2013 C.4.4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	1.1.0 ↗
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0 ↗
Update privacy plan, policies, and procedures ↗	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	1.1.0 ↗

## Leadership

### Leadership and commitment

ID: ISO 27001:2013 C.5.1.a Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Appoint a senior information security officer ↗	CMA_C1733 - Appoint a senior information security officer	Manual, Disabled	1.1.0 ↗
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	1.1.0 ↗
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0 ↗
Update privacy plan, policies, and procedures ↗	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	1.1.0 ↗

## Leadership and commitment

ID: ISO 27001:2013 C.5.1.b Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Appoint a senior information security officer ↗	CMA_C1733 - Appoint a senior information security officer	Manual, Disabled	1.1.0 ↗
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	1.1.0 ↗
Develop audit and accountability policies and procedures ↗	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	1.1.0 ↗
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	1.1.0 ↗
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review access control policies and procedures ↗	CMA_0457 - Review access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update configuration management policies and procedures ↗	CMA_C1175 - Review and update configuration management policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update contingency planning policies and procedures ↗	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update identification and authentication policies and procedures ↗	CMA_C1299 - Review and update identification and authentication policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update incident response policies and procedures ↗	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update information integrity policies and procedures ↗	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update media protection policies and procedures ↗	CMA_C1427 - Review and update media protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update personnel security policies and procedures ↗	CMA_C1507 - Review and update personnel security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update physical and environmental policies and	CMA_C1446 - Review and update physical and environmental policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal) <a href="#">Review and update planning policies and procedures ↗</a>	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	(GitHub) <a href="#">1.1.0 ↗</a>
<a href="#">Review and update risk assessment policies and procedures ↗</a>	CMA_C1537 - Review and update risk assessment policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update system and communications protection policies and procedures ↗</a>	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update system and services acquisition policies and procedures ↗</a>	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update system maintenance policies and procedures ↗</a>	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review security assessment and authorization policies and procedures ↗</a>	CMA_C1143 - Review security assessment and authorization policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update information security policies ↗</a>	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update privacy plan, policies, and procedures ↗</a>	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Leadership and commitment

ID: ISO 27001:2013 C.5.1.c Ownership: Shared

[\[ \]](#) Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Align business objectives and IT goals ↗</a>	CMA_0008 - Align business objectives and IT goals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Allocate resources in determining information system requirements ↗</a>	CMA_C1561 - Allocate resources in determining information system requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Appoint a senior information security officer ↗</a>	CMA_C1733 - Appoint a senior information security officer	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ business case to record the resources required ↗</a>	CMA_C1735 - Employ business case to record the resources required	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Ensure capital planning and investment requests include necessary resources ↗</a>	CMA_C1734 - Ensure capital planning and investment requests include necessary resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Ensure privacy program information is publicly available ↗</a>	CMA_C1867 - Ensure privacy program information is publicly available	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a discrete line item in budgeting documentation ↗</a>	CMA_C1563 - Establish a discrete line item in budgeting documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a privacy program ↗</a>	CMA_0257 - Establish a privacy program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Govern the allocation of resources ↗</a>	CMA_0293 - Govern the allocation of resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Secure commitment from leadership ↗</a>	CMA_0489 - Secure commitment from leadership	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Leadership and commitment

ID: ISO 27001:2013 C.5.1.d Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Appoint a senior information security officer ↗</a>	CMA_C1733 - Appoint a senior information security officer	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Leadership and commitment

ID: ISO 27001:2013 C.5.1.e Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Appoint a senior information security officer ↗	CMA_C1733 - Appoint a senior information security officer	Manual, Disabled	1.1.0 ↗
Define performance metrics ↗	CMA_0124 - Define performance metrics	Manual, Disabled	1.1.0 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	1.1.0 ↗

## Leadership and commitment

ID: ISO 27001:2013 C.5.1.f Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Align business objectives and IT goals ↗	CMA_0008 - Align business objectives and IT goals	Manual, Disabled	1.1.0 ↗
Allocate resources in determining information system requirements ↗	CMA_C1561 - Allocate resources in determining information system requirements	Manual, Disabled	1.1.0 ↗
Appoint a senior information security officer ↗	CMA_C1733 - Appoint a senior information security officer	Manual, Disabled	1.1.0 ↗
Employ business case to record the resources required ↗	CMA_C1735 - Employ business case to record the resources required	Manual, Disabled	1.1.0 ↗
Ensure capital planning and investment requests include necessary resources ↗	CMA_C1734 - Ensure capital planning and investment requests include necessary resources	Manual, Disabled	1.1.0 ↗
Establish a discrete line item in budgeting documentation ↗	CMA_C1563 - Establish a discrete line item in budgeting documentation	Manual, Disabled	1.1.0 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗
Govern the allocation of resources ↗	CMA_0293 - Govern the allocation of resources	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Secure commitment from leadership ↗	CMA_0489 - Secure commitment from leadership	Manual, Disabled	1.1.0 ↗

## Leadership and commitment

ID: ISO 27001:2013 C.5.1.g Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Appoint a senior information security officer ↗	CMA_C1733 - Appoint a senior information security officer	Manual, Disabled	1.1.0 ↗
Define performance metrics ↗	CMA_0124 - Define performance metrics	Manual, Disabled	1.1.0 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	1.1.0 ↗

## Leadership and commitment

ID: ISO 27001:2013 C.5.1.h Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Appoint a senior information security officer ↗	CMA_C1733 - Appoint a senior information security officer	Manual, Disabled	1.1.0 ↗

## Policy

ID: ISO 27001:2013 C.5.2.a Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	1.1.0 ↗
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0 ↗
Update privacy plan, policies, and procedures ↗	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	1.1.0 ↗

## Policy

ID: ISO 27001:2013 C.5.2.b Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	1.1.0 ↗
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0 ↗
Update privacy plan, policies, and procedures ↗	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	1.1.0 ↗

## Policy

ID: ISO 27001:2013 C.5.2.c Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop audit and accountability policies and procedures ↗	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	1.1.0 ↗
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	1.1.0 ↗
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0 ↗
Review access control policies and procedures ↗	CMA_0457 - Review access control policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update configuration management policies and procedures ↗	CMA_C1175 - Review and update configuration management policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update contingency planning policies and procedures ↗	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update identification and authentication policies and procedures ↗	CMA_C1299 - Review and update identification and authentication policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update incident response policies and procedures ↗	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update information integrity policies and procedures ↗	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update media protection policies and procedures ↗	CMA_C1427 - Review and update media protection policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update personnel security policies and procedures ↗	CMA_C1507 - Review and update personnel security policies and procedures	Manual, Disabled	1.1.0 ↗
Review and update physical and environmental policies and	CMA_C1446 - Review and update physical and environmental policies	Manual, Disabled	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal) <a href="#">Review and update planning policies and procedures ↗</a>	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	(GitHub) <a href="#">1.1.0 ↗</a>
<a href="#">Review and update risk assessment policies and procedures ↗</a>	CMA_C1537 - Review and update risk assessment policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update system and communications protection policies and procedures ↗</a>	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update system and services acquisition policies and procedures ↗</a>	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update system maintenance policies and procedures ↗</a>	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review security assessment and authorization policies and procedures ↗</a>	CMA_C1143 - Review security assessment and authorization policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update information security policies ↗</a>	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update privacy plan, policies, and procedures ↗</a>	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Policy

ID: ISO 27001:2013 C.5.2.d Ownership: Shared

[\[ \]](#) Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Develop access control policies and procedures ↗</a>	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop audit and accountability policies and procedures ↗</a>	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop information security policies and procedures ↗</a>	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review access control policies and procedures ↗	CMA_0457 - Review access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update configuration management policies and procedures ↗	CMA_C1175 - Review and update configuration management policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update contingency planning policies and procedures ↗	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update identification and authentication policies and procedures ↗	CMA_C1299 - Review and update identification and authentication policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update incident response policies and procedures ↗	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update information integrity policies and procedures ↗	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update media protection policies and procedures ↗	CMA_C1427 - Review and update media protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update personnel security policies and procedures ↗	CMA_C1507 - Review and update personnel security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update physical and environmental policies and procedures ↗	CMA_C1446 - Review and update physical and environmental policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update planning policies and procedures ↗	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update risk assessment policies and	CMA_C1537 - Review and update risk assessment policies and	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal) <a href="#">Review and update system and communications protection policies and procedures ↗</a>	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	(GitHub) <a href="#">1.1.0 ↗</a>
<a href="#">Review and update system and services acquisition policies and procedures ↗</a>	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update system maintenance policies and procedures ↗</a>	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review security assessment and authorization policies and procedures ↗</a>	CMA_C1143 - Review security assessment and authorization policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update information security policies ↗</a>	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update privacy plan, policies, and procedures ↗</a>	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Policy

ID: ISO 27001:2013 C.5.2.e Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Develop access control policies and procedures ↗</a>	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document security and privacy training activities ↗</a>	CMA_0198 - Document security and privacy training activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Govern policies and procedures ↗</a>	CMA_0292 - Govern policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update privacy plan, policies, and procedures ↗</a>	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Policy

ID: ISO 27001:2013 C.5.2.f Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update privacy plan, policies, and procedures ↗	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Policy

ID: ISO 27001:2013 C.5.2.g Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Update privacy plan, policies, and procedures ↗	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Organizational roles, responsibilities and authorities

ID: ISO 27001:2013 C.5.3.b Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define performance metrics ↗	CMA_0124 - Define performance metrics	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Planning

## General

ID: ISO 27001:2013 C.6.1.1.a Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop POA&amp;M ↗</a>	CMA_C1156 - Develop POA&M	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a risk management strategy ↗</a>	CMA_0258 - Establish a risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement the risk management strategy ↗</a>	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## General

ID: ISO 27001:2013 C.6.1.1.b Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop POA&amp;M ↗</a>	CMA_C1156 - Develop POA&M	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a risk management strategy ↗</a>	CMA_0258 - Establish a risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement the risk management strategy ↗</a>	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## General

ID: ISO 27001:2013 C.6.1.1.c Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop POA&M ↗	CMA_C1156 - Develop POA&M	Manual, Disabled	1.1.0 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗
Implement the risk management strategy ↗	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	1.1.0 ↗

## General

ID: ISO 27001:2013 C.6.1.1.d Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop POA&M ↗	CMA_C1156 - Develop POA&M	Manual, Disabled	1.1.0 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗
Implement the risk management strategy ↗	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	1.1.0 ↗

## General

ID: ISO 27001:2013 C.6.1.1.e.1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop POA&M ↗	CMA_C1156 - Develop POA&M	Manual, Disabled	1.1.0 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗
Implement the risk management strategy ↗	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	1.1.0 ↗

## General

ID: ISO 27001:2013 C.6.1.1.e.2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish a risk management strategy ↗</a>	CMA_0258 - Establish a risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement the risk management strategy ↗</a>	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update POA&amp;M items ↗</a>	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information security risk assessment

ID: ISO 27001:2013 C.6.1.2.a.1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish a risk management strategy ↗</a>	CMA_0258 - Establish a risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement the risk management strategy ↗</a>	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information security risk assessment

ID: ISO 27001:2013 C.6.1.2.a.2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish a risk management strategy ↗</a>	CMA_0258 - Establish a risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement the risk management strategy ↗	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	1.1.0 ↗

## Information security risk assessment

ID: ISO 27001:2013 C.6.1.2.b Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement the risk management strategy ↗	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	1.1.0 ↗

## Information security risk assessment

ID: ISO 27001:2013 C.6.1.2.c.1 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement the risk management strategy ↗	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	1.1.0 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	1.1.0 ↗

## Information security risk assessment

ID: ISO 27001:2013 C.6.1.2.c.2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement the risk management strategy ↗	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Perform a risk assessment ↗</a>	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information security risk assessment

ID: ISO 27001:2013 C.6.1.2.d.1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement the risk management strategy ↗</a>	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a risk assessment ↗</a>	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information security risk assessment

ID: ISO 27001:2013 C.6.1.2.d.2 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement the risk management strategy ↗</a>	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a risk assessment ↗</a>	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information security risk assessment

ID: ISO 27001:2013 C.6.1.2.d.3 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement the risk management strategy ↗</a>	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a risk assessment ↗</a>	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information security risk assessment

ID: ISO 27001:2013 C.6.1.2.e.1 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement the risk management strategy ↗</a>	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a risk assessment ↗</a>	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information security risk assessment

ID: ISO 27001:2013 C.6.1.2.e.2 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement the risk management strategy ↗</a>	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a risk assessment ↗</a>	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information security risk treatment

ID: ISO 27001:2013 C.6.1.3.a Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop POA&M ↗	CMA_C1156 - Develop POA&M	Manual, Disabled	1.1.0 ↗

## Information security risk treatment

ID: ISO 27001:2013 C.6.1.3.b Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop POA&M ↗	CMA_C1156 - Develop POA&M	Manual, Disabled	1.1.0 ↗

## Information security risk treatment

ID: ISO 27001:2013 C.6.1.3.c Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop POA&M ↗	CMA_C1156 - Develop POA&M	Manual, Disabled	1.1.0 ↗

## Information security risk treatment

ID: ISO 27001:2013 C.6.1.3.d Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop SSP that meets criteria ↗	CMA_C1492 - Develop SSP that meets criteria	Manual, Disabled	1.1.0 ↗

## Information security risk treatment

ID: ISO 27001:2013 C.6.1.3.e Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop POA&amp;M ↗</a>	CMA_C1156 - Develop POA&M	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information security risk treatment

ID: ISO 27001:2013 C.6.1.3.f Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop POA&amp;M ↗</a>	CMA_C1156 - Develop POA&M	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information security objectives and planning to achieve them

ID: ISO 27001:2013 C.6.2.e Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish an information security program ↗</a>	CMA_0263 - Establish an information security program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update information security policies ↗</a>	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Support

### Resources

ID: ISO 27001:2013 C.7.1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Align business objectives and IT goals ↗	CMA_0008 - Align business objectives and IT goals	Manual, Disabled	1.1.0 ↗
Allocate resources in determining information system requirements ↗	CMA_C1561 - Allocate resources in determining information system requirements	Manual, Disabled	1.1.0 ↗
Employ business case to record the resources required ↗	CMA_C1735 - Employ business case to record the resources required	Manual, Disabled	1.1.0 ↗
Ensure capital planning and investment requests include necessary resources ↗	CMA_C1734 - Ensure capital planning and investment requests include necessary resources	Manual, Disabled	1.1.0 ↗
Establish a discrete line item in budgeting documentation ↗	CMA_C1563 - Establish a discrete line item in budgeting documentation	Manual, Disabled	1.1.0 ↗
Govern the allocation of resources ↗	CMA_0293 - Govern the allocation of resources	Manual, Disabled	1.1.0 ↗
Secure commitment from leadership ↗	CMA_0489 - Secure commitment from leadership	Manual, Disabled	1.1.0 ↗

## Competence

ID: ISO 27001:2013 C.7.2.a Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	Manual, Disabled	1.1.0 ↗
Monitor security and privacy training completion ↗	CMA_0379 - Monitor security and privacy training completion	Manual, Disabled	1.1.0 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗

## Competence

ID: ISO 27001:2013 C.7.2.b Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Monitor security and privacy training completion ↗</a>	CMA_0379 - Monitor security and privacy training completion	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Competence

ID: ISO 27001:2013 C.7.2.c Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Monitor security and privacy training completion ↗</a>	CMA_0379 - Monitor security and privacy training completion	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Competence

ID: ISO 27001:2013 C.7.2.d Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Retain training records ↗</a>	CMA_0456 - Retain training records	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Awareness

ID: ISO 27001:2013 C.7.3.a Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop acceptable use policies and procedures ↗</a>	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce rules of behavior and</a>	CMA_0248 - Enforce rules of	Manual,	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">access agreements ↗</a>	behavior and access agreements	Disabled	
<a href="#">Provide privacy training ↗</a>	CMA_0415 - Provide privacy training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Awareness

ID: ISO 27001:2013 C.7.3.b Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop acceptable use policies and procedures ↗</a>	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce rules of behavior and access agreements ↗</a>	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Provide privacy training ↗</a>	CMA_0415 - Provide privacy training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Awareness

ID: ISO 27001:2013 C.7.3.c Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop acceptable use policies and procedures ↗</a>	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce rules of behavior and access agreements ↗</a>	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Provide privacy training ↗</a>	CMA_0415 - Provide privacy training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Communication

ID: ISO 27001:2013 C.7.4.a Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Designate authorized personnel to post publicly accessible information ↗	CMA_C1083 - Designate authorized personnel to post publicly accessible information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Communication

ID: ISO 27001:2013 C.7.4.b Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Designate authorized personnel to post publicly accessible information ↗	CMA_C1083 - Designate authorized personnel to post publicly accessible information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Communication

ID: ISO 27001:2013 C.7.4.c Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Designate authorized personnel to post publicly accessible information ↗	CMA_C1083 - Designate authorized personnel to post publicly accessible information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Communication

ID: ISO 27001:2013 C.7.4.d Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Designate authorized personnel to post publicly accessible information ↗	CMA_C1083 - Designate authorized personnel to post publicly accessible information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Communication

ID: ISO 27001:2013 C.7.4.e Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Designate authorized personnel to post publicly accessible information ↗	CMA_C1083 - Designate authorized personnel to post publicly accessible information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Creating and updating

ID: ISO 27001:2013 C.7.5.2.c Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop SSP that meets criteria ↗	CMA_C1492 - Develop SSP that meets criteria	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Control of documented information

ID: ISO 27001:2013 C.7.5.3.a Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update planning policies and procedures ↗	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Control of documented information

ID: ISO 27001:2013 C.7.5.3.b Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop and establish a system security plan ↗</a>	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish security requirements for the manufacturing of connected devices ↗</a>	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement security engineering principles of information systems ↗</a>	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Control of documented information

ID: ISO 27001:2013 C.7.5.3.c Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update planning policies and procedures ↗</a>	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Control of documented information

ID: ISO 27001:2013 C.7.5.3.d Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop and establish a system security plan ↗</a>	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish security requirements for the manufacturing of</a>	CMA_0279 - Establish security requirements for the manufacturing	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal) Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗

## Control of documented information

ID: ISO 27001:2013 C.7.5.3.e Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	1.1.0 ↗
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	1.1.0 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗

## Control of documented information

ID: ISO 27001:2013 C.7.5.3.f Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗
Establish security requirements for the manufacturing of	CMA_0279 - Establish security requirements for the manufacturing	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">connected devices ↗</a>	of connected devices		
<a href="#">Implement security engineering principles of information systems ↗</a>	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform audit for configuration change control ↗</a>	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update planning policies and procedures ↗</a>	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Operation

## Operational planning and control

ID: ISO 27001:2013 C.8.1 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Automate approval request for proposed changes ↗</a>	CMA_C1192 - Automate approval request for proposed changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate implementation of approved change notifications ↗</a>	CMA_C1196 - Automate implementation of approved change notifications	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate process to document implemented changes ↗</a>	CMA_C1195 - Automate process to document implemented changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate process to highlight unreviewed change proposals ↗</a>	CMA_C1193 - Automate process to highlight unreviewed change proposals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate process to prohibit implementation of unapproved changes ↗</a>	CMA_C1194 - Automate process to prohibit implementation of unapproved changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate proposed documented changes ↗</a>	CMA_C1191 - Automate proposed documented changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop and maintain a vulnerability management standard ↗	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop POA&M ↗	CMA_C1156 - Develop POA&M	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to document approved changes and potential impact ↗	CMA_C1597 - Require developers to document approved changes and potential impact	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to implement only approved changes ↗	CMA_C1596 - Require developers to implement only approved changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to manage change integrity ↗	CMA_C1595 - Require developers to manage change integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require external service providers to comply with security requirements ↗	CMA_C1586 - Require external service providers to comply with security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update POA&M items ↗	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Information security risk assessment

ID: ISO 27001:2013 C.8.2 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
Conduct risk assessment and document its results ↗	CMA_C1542 - Conduct risk assessment and document its results	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and update risk assessment policies and procedures ↗	CMA_C1537 - Review and update risk assessment policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Information security risk treatment

ID: ISO 27001:2013 C.8.3 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
Develop POA&M ↗	CMA_C1156 - Develop POA&M	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update POA&M items ↗	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Performance Evaluation

## Monitoring, measurement, analysis and evaluation

ID: ISO 27001:2013 C.9.1.a Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure detection whitelist ↗	CMA_0068 - Configure detection whitelist	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Turn on sensors for endpoint security solution ↗	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Monitoring, measurement, analysis and evaluation

ID: ISO 27001:2013 C.9.1.b Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure detection whitelist ↗	CMA_0068 - Configure detection whitelist	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Turn on sensors for endpoint security solution ↗	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Monitoring, measurement, analysis and evaluation

ID: ISO 27001:2013 C.9.1.c Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure detection whitelist ↗	CMA_0068 - Configure detection whitelist	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Turn on sensors for endpoint security solution ↗	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Undergo independent security review ↗</a>	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Monitoring, measurement, analysis and evaluation

ID: ISO 27001:2013 C.9.1.d Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Configure detection whitelist ↗</a>	CMA_0068 - Configure detection whitelist	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Turn on sensors for endpoint security solution ↗</a>	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Undergo independent security review ↗</a>	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Monitoring, measurement, analysis and evaluation

ID: ISO 27001:2013 C.9.1.e Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Configure detection whitelist ↗</a>	CMA_0068 - Configure detection whitelist	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Turn on sensors for endpoint security solution ↗</a>	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Undergo independent security review ↗</a>	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Monitoring, measurement, analysis and evaluation

ID: ISO 27001:2013 C.9.1.f Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure detection whitelist ↗	CMA_0068 - Configure detection whitelist	Manual, Disabled	1.1.0 ↗
Turn on sensors for endpoint security solution ↗	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	1.1.0 ↗
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	1.1.0 ↗

## Internal audit

ID: ISO 27001:2013 C.9.2.a.1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop security assessment plan ↗	CMA_C1144 - Develop security assessment plan	Manual, Disabled	1.1.0 ↗

## Internal audit

ID: ISO 27001:2013 C.9.2.a.2 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop security assessment plan ↗	CMA_C1144 - Develop security assessment plan	Manual, Disabled	1.1.0 ↗

## Internal audit

ID: ISO 27001:2013 C.9.2.b Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop security assessment plan ↗	CMA_C1144 - Develop security assessment plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Internal audit

ID: ISO 27001:2013 C.9.2.c Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess Security Controls ↗	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop security assessment plan ↗	CMA_C1144 - Develop security assessment plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Internal audit

ID: ISO 27001:2013 C.9.2.d Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop security assessment plan ↗	CMA_C1144 - Develop security assessment plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Internal audit

ID: ISO 27001:2013 C.9.2.e Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adjust level of audit review, analysis, and reporting ↗	CMA_C1123 - Adjust level of audit review, analysis, and reporting	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop audit and accountability policies and procedures ↗	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	1.1.0 ↗
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	1.1.0 ↗
Employ independent assessors to conduct security control assessments ↗	CMA_C1148 - Employ independent assessors to conduct security control assessments	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗

## Internal audit

ID: ISO 27001:2013 C.9.2.f Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Deliver security assessment results ↗	CMA_C1147 - Deliver security assessment results	Manual, Disabled	1.1.0 ↗

## Internal audit

ID: ISO 27001:2013 C.9.2.g Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adhere to retention periods defined ↗	CMA_0004 - Adhere to retention periods defined	Manual, Disabled	1.1.0 ↗
Retain security policies and procedures ↗	CMA_0454 - Retain security policies and procedures	Manual, Disabled	1.1.0 ↗
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	1.1.0 ↗

## Management review

ID: ISO 27001:2013 C.9.3.a Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Assess Security Controls ↗</a>	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct Risk Assessment ↗</a>	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop POA&amp;M ↗</a>	CMA_C1156 - Develop POA&M	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement plans of action and milestones for security program process ↗</a>	CMA_C1737 - Implement plans of action and milestones for security program process	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update POA&amp;M items ↗</a>	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Management review

ID: ISO 27001:2013 C.9.3.b Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Assess Security Controls ↗</a>	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct Risk Assessment ↗</a>	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop POA&amp;M ↗</a>	CMA_C1156 - Develop POA&M	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update POA&amp;M items ↗</a>	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Management review

ID: ISO 27001:2013 C.9.3.c.1 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess Security Controls ↗</a>	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct Risk Assessment ↗</a>	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define performance metrics ↗</a>	CMA_0124 - Define performance metrics	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop POA&amp;M ↗</a>	CMA_C1156 - Develop POA&M	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish an information security program ↗</a>	CMA_0263 - Establish an information security program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update POA&amp;M items ↗</a>	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Management review

ID: ISO 27001:2013 C.9.3.c.2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess Security Controls ↗</a>	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct Risk Assessment ↗</a>	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop POA&amp;M ↗</a>	CMA_C1156 - Develop POA&M	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update POA&amp;M items ↗</a>	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Management review

ID: ISO 27001:2013 C.9.3.c.3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess Security Controls ↗</a>	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct Risk Assessment ↗</a>	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define performance metrics ↗</a>	CMA_0124 - Define performance metrics	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update POA&amp;M items ↗</a>	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Management review

ID: ISO 27001:2013 C.9.3.c.4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess Security Controls ↗</a>	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct Risk Assessment ↗</a>	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define performance metrics ↗</a>	CMA_0124 - Define performance metrics	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update POA&amp;M items ↗</a>	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Management review

ID: ISO 27001:2013 C.9.3.d Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess Security Controls ↗</a>	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct Risk Assessment ↗</a>	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update POA&amp;M items ↗</a>	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Management review

ID: ISO 27001:2013 C.9.3.e Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess Security Controls ↗</a>	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct Risk Assessment ↗</a>	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update POA&amp;M items ↗</a>	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Management review

ID: ISO 27001:2013 C.9.3.f Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess Security Controls ↗</a>	CMA_C1145 - Assess Security Controls	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct Risk Assessment ↗</a>	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update POA&amp;M items ↗</a>	CMA_C1157 - Update POA&M items	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Next steps

Additional articles about Azure Policy:

- Regulatory Compliance overview.
- See the initiative definition structure.
- Review other examples at [Azure Policy samples](#).
- Review [Understanding policy effects](#).
- Learn how to [remediate non-compliant resources](#).

# International Traffic in Arms Regulations (ITAR)

Article • 09/25/2022

## ITAR overview

The US Department of State has export control authority over defense articles, services, and related technologies under the [International Traffic in Arms Regulations](#) (ITAR) managed by the [Directorate of Defense Trade Controls](#) (DDTC). Items under ITAR protection are documented on the [United States Munitions List](#) (USML). If you're a manufacturer, exporter, and broker of defense articles, services, and related technologies as defined on the USML, you must be registered with DDTC, must understand and abide by ITAR, and must self-certify that you operate in accordance with ITAR.

DDTC [revised the ITAR rules](#) effective 25 March 2020 to align them more closely with the Export Administration Regulations (EAR). These ITAR revisions introduced an end-to-end data encryption carve-out that incorporated many of the same terms that the US Department of Commerce adopted in 2016 for the EAR. Specifically, the revised ITAR rules state that activities that don't constitute exports, re-exports, re-transfers, or temporary imports include (among other activities) the sending, taking, or storing of technical data that is 1) unclassified, 2) secured using end-to-end encryption, 3) secured using FIPS 140 compliant cryptographic modules as prescribed in the regulations, 4) not intentionally sent to a person in or stored in a [country proscribed in § 126.1](#) or the Russian Federation, and 5) not sent from a country proscribed in § 126.1 or the Russian Federation. Moreover, DDTC clarified that data in-transit via the Internet isn't deemed to be stored. End-to-end encryption implies the data is kept encrypted at all times between the originator and intended recipient, and the means of decryption aren't provided to any third party.

## Azure and ITAR

There is no ITAR compliance certification. However, if you're subject to ITAR, Azure, Azure Government, and Azure Government Secret can help you meet your ITAR compliance requirements.

Except for the Azure region in Hong Kong SAR, Azure datacenters aren't located in proscribed countries or in the Russian Federation. Azure services rely on [FIPS 140](#)

validated cryptographic modules in the underlying operating system, and provide you with [many options for encrypting data](#) in transit and at rest, including encryption key management using [Azure Key Vault](#). The Key Vault service can store encryption keys in FIPS 140 validated hardware security modules (HSMs) under your control, also known as [customer-managed keys \(CMK\)](#). Keys generated inside the Azure Key Vault HSMs aren't exportable – there can be no clear-text version of the key outside the HSMs. This binding is enforced by the underlying HSM. **Azure Key Vault is designed, deployed, and operated such that Microsoft and its agents don't see or extract your cryptographic keys.** For more information, see [How does Azure Key Vault protect your keys?](#)

 **Note**

You're responsible for choosing the Azure regions for deploying your applications and data. Moreover, you're responsible for designing your applications to use end-to-end data encryption that meets ITAR requirements. Microsoft doesn't inspect, approve, or monitor your Azure applications.

Azure Government provides an extra layer of protection to customers through contractual commitments regarding storage of customer data in the United States and limiting potential access to systems processing customer data to [screened US persons](#).

For more information regarding ITAR, you should review:

- [Azure export controls](#) online documentation
- [Microsoft Azure Export Controls](#) whitepaper

## Applicability

- Azure
- Azure Government
- Azure Government Secret

## Office 365 and ITAR

For more information about Office 365 compliance, see [Office 365 ITAR documentation](#).

## Frequently asked questions

**What should I do to comply with export control laws when using Azure?**

If you're a manufacturer, exporter, and broker of defense articles, services, and related

technologies as defined on the USML, you must be registered with DDTC, must understand and abide by ITAR, and must self-certify that you operate in accordance with ITAR. You must carefully assess how your use of Azure may implicate US export controls and determine whether any of the data you want to use or store there may be subject to ITAR controls, and if so, what controls apply. To learn more about how Azure can help you ensure your full compliance with US export controls, review the [Microsoft Azure Export Controls](#) whitepaper.

## What technical features does Azure provide to help customers meet their ITAR compliance obligations?

The following Azure features are available to you to manage potential export control risks:

- **Ability to control data location** – You have visibility as to where your data is stored, and robust tools to restrict data storage to a single geography, region, or country. For example, you may therefore ensure that data is stored in the United States or your country of choice and minimize transfer of controlled technology/technical data outside the target country. Customer data isn't *intentionally stored* in a non-conforming location, consistent with the ITAR rules.
- **Control over access to data** – You can know and control who can access your data and on what terms. Microsoft technical support personnel don't need and don't have default access to customer data. For those rare instances where resolving customer support requests requires elevated access to customer data, [Customer Lockbox for Azure](#) puts you in charge of approving or rejecting customer data access requests.
- **End-to-end encryption** – Implies the data is kept encrypted at all times between the originator and intended recipient, and the means of decryption aren't provided to any third party. Azure relies on [FIPS 140](#) validated cryptographic modules in the underlying operating system, and provides you with [many options for encrypting data](#) in transit and at rest, including encryption key management using [Azure Key Vault](#). The Key Vault service can store encryption keys in FIPS 140 validated hardware security modules (HSMs) under your control, also known as [customer-managed keys \(CMK\)](#). Azure Key Vault is designed, deployed, and operated such that Microsoft and its agents [don't see or extract your cryptographic keys](#).
- **Tools and protocols to prevent unauthorized deemed export/re-export** – Apart from the ITAR *end-to-end encryption* safe harbor for physical storage locations, the use of encryption also helps protect against a potential deemed export (or deemed re-export), because even if a non-US person has access to the encrypted data, nothing is actually revealed to non-US person who can't read or understand the data while it is encrypted and thus there is no *release* of any controlled data. However, ITAR requires some authorization before granting foreign persons with

access information that would enable them to decrypt ITAR technical data. Azure offers a wide range of encryption capabilities and solutions, flexibility to choose among encryption options, and robust tools for managing encryption.

### **Are Microsoft technologies, products, and services subject to ITAR?**

In general, Microsoft technologies, products, and services aren't subject to ITAR and aren't listed on the [United States Munitions List](#) (USML).

### **What's the difference between ITAR and the Export Administration Regulations (EAR)?**

The primary US export controls with the broadest application are the EAR, administered by the US Department of Commerce. The EAR is applicable to dual-use items that have both commercial and military applications, and to items with purely commercial applications.

The United States also has separate and more specialized export control regulations, such as the ITAR, that governs the most sensitive items and technology. Administered by the US Department of State, ITAR imposes controls on the export, temporary import, re-export, and transfer of many military, defense, and intelligence items – also known as *defense articles* – including related technical data documented on the [United States Munitions List](#) (USML).

### **Should I use Azure or Azure Government for workloads that are subject to ITAR?**

You're wholly responsible for ensuring your own compliance with all applicable laws and regulations and should consult your legal advisor for questions regarding regulatory compliance. Azure and Azure Government have the same security controls in place, including the same provisions for data encryption in transit and at rest to support ITAR requirements. The cloud environment decision will rest with you based on your business requirements. Most US government agencies and their partners are best aligned with Azure Government, which provides an extra layer of protection to customers through contractual commitments regarding storage of customer data in the United States and limiting potential access to systems processing customer data to [screened US persons](#).

## **Resources**

- [Azure compliance documentation](#)
- [Azure enables a world of compliance](#)
- [Microsoft 365 compliance offerings](#)
- [Compliance on the Microsoft Trust Center](#)
- [What is Azure Government?](#)
- [Explore Azure Government](#)
- [Microsoft government solutions](#)
- [Azure support for export controls](#)

- Microsoft Azure Export Controls  whitepaper
- DDTC ITAR landing page 
- ITAR Title 22 CFR Part 120-130 
- United States Munitions List  (USML)
- DDTC revised ITAR rule  effective 25 March 2020
- Title 22 CFR Part 126.1  proscribed countries

# Joint Special Access Program (SAP) Implementation Guide (JSIG)

Article • 05/06/2023

## JSIG overview

Special Access Programs represent some of the US Department of Defense (DoD) most sensitive information that must be protected accordingly. Given the rapid increase in cybersecurity threats, DoD can no longer rely on physical isolation as a primary risk mitigation strategy. Instead, the National Institute of Standards and Technology (NIST) [SP 800-37](#) provides a common information security framework for the US federal government and its contractors to improve information security, strengthen risk management processes, and transform the traditional certification and accreditation process into a modern Risk Management Framework (RMF). The [DoDM 5205.07](#), Volume 1, *Special Access Program (SAP) Security Manual: General Procedures*, provides policy, guidance, and standards for the authorization of information systems and application of RMF within a DoD SAP.

The purpose of the [Joint Special Access Program \(SAP\) Implementation Guide \(JSIG\)](#) is to provide policy and guidance on the implementation of the RMF. JSIG serves as a technical supplement to [NIST SP 800-53](#) and [CNSSI 1253](#). It is used in combination with the applicable volume of DoDM 5205.07 in the application of the RMF. JSIG provides standardized policies for cybersecurity and information assurance, procedures, and implementation guidance for use in the management of systems at all classification levels under the purview of the SAP Authorizing Official (AO). These policies and procedures adhere to applicable laws, executive orders, directives, policies, regulations, standards, and guidance.

## Azure and JSIG

Azure Government Secret and Azure Government Top Secret maintain JSIG Authorizations to Operate (ATO) at Protection Level 3 (PL3).

[Azure Government Secret](#) was developed using the same principles and architecture as Azure commercial cloud. It enables fast access to sensitive, mission-critical information while maintaining the security and integrity of classified workloads. It is available from three dedicated regions located over 500 miles apart. Azure Government

Secret operates on secure, native connections to classified networks with options for [ExpressRoute](#) and [ExpressRoute Direct](#) for private, resilient, high-bandwidth connectivity.

[Azure Government Top Secret](#) serves the national security mission and empowers leaders across the Intelligence Community (IC), Department of Defense (DoD), and Federal Civilian agencies to process national security workloads classified at the US Top Secret level. Azure regions for Top Secret classified data expand the ability of our national security customers to achieve greater agility, cost savings, and speed to innovation.

## Applicability

- Azure Government Secret
- Azure Government Top Secret

## Services in scope

For a list of Microsoft cloud services in scope for the JSIG ATO in Azure Government Secret or Azure Government Top Secret, contact your Microsoft account representative.

## Attestation documents

Contact your Microsoft account representative for assistance.

## Frequently asked questions

### What Azure services are covered by the JSIG Authorization to Operate (ATO)?

For a list of Microsoft online services in scope for the JSIG ATO in Azure Government Secret or Azure Government Top Secret, contact your Microsoft account representative.

## Resources

- [Azure compliance documentation](#)
- [Azure enables a world of compliance](#)
- [Microsoft 365 compliance offerings](#)
- [Compliance on the Microsoft Trust Center](#)
- [Azure for US Government](#)
- [Azure Government Secret](#)
- [Azure Government Top Secret](#)

- [DoDM 5205.07 Special Access Program \(SAP\) Security Manual, Volumes 1 - 4](#)
- [DoD Instruction 8510.01](#) *DoD Risk Management Framework (RMF) for DoD Information Technology (IT)*
- [DoD Joint Special Access Program \(SAP\) Implementation Guide \(JSIG\)](#)
- [DoD SAP Program Manager's Handbook to the JSIG and RMF](#)
- [NIST SP 800-30](#) *Guide for Conducting Risk Assessments*
- [NIST SP 800-37](#) *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- [NIST SP 800-39](#) *Managing Information Security Risk: Organization, Mission, and Information System View*
- [NIST SP 800-53](#) *Security and Privacy Controls for Information Systems and Organizations*
- [NIST SP 800-59](#) *Guideline for Identifying an Information System as a National Security System*
- [CNSSI 1253](#) *Security Categorization and Control Selection for National Security Systems*

# National Defense Authorization Act (NDAA)

Article • 10/10/2022

## NDAA Section 889 overview

Section 889 of the [2019 National Defense Authorization Act](#) (NDAA) prohibits US federal government agencies, contractors, and grant and loan recipients from procuring or using *certain covered telecommunications equipment and services* as described in the statute. NDAA Section 889 seeks to mitigate privacy and security risks to US government by prohibiting the purchase and use of such equipment. These prohibitions were implemented in two phases:

- **Section 889(a)(1)(A)** prohibits federal agencies from purchasing covered telecommunications equipment and services. It became effective on 13 August 2019. The US Department of Defense (DoD), General Services Administration (GSA), and National Aeronautics and Space Administration (NASA) issued two interim rules amending the Federal Acquisition Regulation (FAR) to implement Section 889(a)(1)(A). For more information, see [interim rule 1](#) and [interim rule 2](#).
- **Section 889(a)(1)(B)** prohibits federal agencies from entering into, or extending or renewing, a contract with a company that uses covered telecommunications equipment and services. It became effective on 13 August 2020, and it has much broader scope than the first phase. It's aimed at ensuring that US government doesn't conduct business with companies that use covered telecommunications equipment and services. DoD, GSA, and NASA issued an [interim rule](#) amending the FAR to implement Section 889(a)(1)(B).

The detailed definition of *covered telecommunications equipment and services* is provided in the statute as follows:

- (A) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).
- (B) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).

- (C) Telecommunications or video surveillance services provided by such entities or using such equipment.
- (D) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

## Microsoft support for NDAA Section 889

For purposes of NDAA Section 889(a)(1)(B), Microsoft understands that its partners and customers are conducting “reasonable inquiries” regarding their use of prohibited covered telecommunications equipment and services. Microsoft Azure, Office 365, Dynamics 365, and Surface current products and services offerings in the United States don't use equipment or services of **Huawei Technologies Company**, **ZTE Corporation**, **Hytera Communications Corporation**, **Hangzhou Hikvision Digital Technology Company**, or **Dahua Technology Company**.

## NDAA Section 1634 overview

On 15 June 2018, DoD, GSA, and NASA published an interim rule in the Federal Register to revise the FAR to implement section 1634 of Division A of the NDAA, which prohibits the use of products and services of Kaspersky Lab and its related entities by the Federal Government. Among other things, the interim rule added a corresponding contract clause at [52.204-23](#) that must be included by contracting officers in solicitations issued on or after 16 July 2018, and in resulting contracts.

## Microsoft support for NDAA Section 1634

For purposes of FAR 52.204-23, Microsoft cloud services, including Azure, Dynamics 365, Microsoft 365, and Power Platform, don't use any hardware, software, or services provided by **Kaspersky Lab**.

## Frequently asked questions

### What are covered telecommunications equipment and services?

Detailed definitions are provided in the [2019 National Defense Authorization Act](#) (NDAA), as mentioned in the Overview section previously.

## Does FedRAMP require compliance with Section 889 of the NDAA?

Yes. Effective 20 May 2021, the FedRAMP Joint Authorization Board (JAB) [updated the SA-04 control parameter](#) within the Low, Moderate, and High baselines, specifying that the cloud service providers must comply with Section 889 of the NDAA. Control [SA-04 Acquisition Process](#) is part of the System and Services Acquisition (SA) control family. Both Azure and Azure Government maintain a [FedRAMP High](#) Provisional Authorization to Operate (P-ATO) issued by the JAB.

## Do NDAA Section 889 assurances apply to Microsoft online services outside the United States?

No. The commitment exists only for service offerings in the United States. NDAA Section 889 restrictions are applicable only to procurement by US federal government agencies, contractors, and grant loan recipients.

## Resources

- [Azure compliance documentation](#)
- [Azure enables a world of compliance](#)
- [Microsoft 365 compliance offerings](#)
- [Compliance on the Microsoft Trust Center](#)
- [2019 National Defense Authorization Act](#) (NDAA)
- Section 889(a)(1)(A): DoD, GSA, and NASA [interim rule 1](#) and [interim rule 2](#)
- Section 889(a)(1)(B): DoD, GSA, and NASA [interim rule](#)
- FAR: Use of products and services of Kaspersky Lab, [interim rule](#)
- FAR: Use of products and services of Kaspersky Lab, [final rule](#)
- Microsoft [Product Terms](#) (formerly Online Services Terms)
- Microsoft Products and Services [Data Protection Addendum](#) (DPA)
- [Azure NIST SP 800-161 documentation](#) for supply chain risk management

# Details of the NIST SP 800-53 Rev. 4 Regulatory Compliance built-in initiative

Article • 01/02/2024

The following article details how the Azure Policy Regulatory Compliance built-in initiative definition maps to **compliance domains** and **controls** in NIST SP 800-53 Rev. 4. For more information about this compliance standard, see [NIST SP 800-53 Rev. 4](#). To understand *Ownership*, see [Azure Policy policy definition](#) and [Shared responsibility in the cloud](#).

The following mappings are to the **NIST SP 800-53 Rev. 4** controls. Many of the controls are implemented with an [Azure Policy](#) initiative definition. To review the complete initiative definition, open **Policy** in the Azure portal and select the **Definitions** page. Then, find and select the **NIST SP 800-53 Rev. 4** Regulatory Compliance built-in initiative definition.

## Important

Each control below is associated with one or more [Azure Policy](#) definitions. These policies may help you [assess compliance](#) with the control; however, there often is not a one-to-one or complete match between a control and one or more policies. As such, **Compliant** in Azure Policy refers only to the policy definitions themselves; this doesn't ensure you're fully compliant with all requirements of a control. In addition, the compliance standard includes controls that aren't addressed by any Azure Policy definitions at this time. Therefore, compliance in Azure Policy is only a partial view of your overall compliance status. The associations between compliance domains, controls, and Azure Policy definitions for this compliance standard may change over time. To view the change history, see the [GitHub Commit History](#).

## Access Control

### Access Control Policy And Procedures

ID: NIST SP 800-53 Rev. 4 AC-1 Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review access control policies and procedures ↗	CMA_0457 - Review access control policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Account Management

ID: NIST SP 800-53 Rev. 4 AC-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
A maximum of 3 owners should be designated for your subscription ↗	It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
An Azure Active Directory administrator should be provisioned for SQL servers ↗	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
App Service apps should use managed identity ↗	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Assign account managers ↗	CMA_0015 - Assign account managers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Audit usage of custom RBAC roles ↗	Audit built-in roles such as 'Owner, Contributer, Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and	Audit, Disabled	<a href="#">1.0.1 ↗</a>

<b>Name</b>  (Azure portal)	<b>Description</b>	<b>Effect(s)</b>	<b>Version</b>  (GitHub)
	requires a rigorous review and threat modeling		
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	1.1.0 ↗
<a href="#">Blocked accounts with owner permissions on Azure resources should be removed ↗</a>	Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in.	AuditIfExists, Disabled	1.0.0 ↗
<a href="#">Blocked accounts with read and write permissions on Azure resources should be removed ↗</a>	Deprecated accounts should be removed from your subscriptions. Deprecated accounts are accounts that have been blocked from signing in.	AuditIfExists, Disabled	1.0.0 ↗
<a href="#">Cognitive Services accounts should have local authentication methods disabled ↗</a>	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
<a href="#">Define and enforce conditions for shared and group accounts ↗</a>	CMA_0117 - Define and enforce conditions for shared and group accounts	Manual, Disabled	1.1.0 ↗
<a href="#">Define information system account types ↗</a>	CMA_0121 - Define information system account types	Manual, Disabled	1.1.0 ↗
<a href="#">Document access privileges ↗</a>	CMA_0186 - Document access privileges	Manual, Disabled	1.1.0 ↗
<a href="#">Establish conditions for role membership ↗</a>	CMA_0269 - Establish conditions for role membership	Manual, Disabled	1.1.0 ↗
<a href="#">Function apps should use managed identity ↗</a>	Use a managed identity for enhanced authentication security	AuditIfExists, Disabled	3.0.0 ↗
<a href="#">Guest accounts with owner permissions on Azure resources should be removed ↗</a>	External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access.	AuditIfExists, Disabled	1.0.0 ↗
<a href="#">Guest accounts with read permissions on</a>	External accounts with read privileges should be removed from your subscription in order to prevent unmonitored access.	AuditIfExists, Disabled	1.0.0 ↗

Azure resources	Description	Effect(s)	Version (GitHub)
<a href="#">Name should be removed (Azure portal)</a>			
<a href="#">Guest accounts with write permissions on Azure resources should be removed</a>	External accounts with write privileges should be removed from your subscription in order to prevent unmonitored access.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Monitor account activity</a>	CMA_0377 - Monitor account activity	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Notify Account Managers of customer controlled accounts</a>	CMA_C1009 - Notify Account Managers of customer controlled accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Reissue authenticators for changed groups and accounts</a>	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require approval for account creation</a>	CMA_0431 - Require approval for account creation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Restrict access to privileged accounts</a>	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review account provisioning logs</a>	CMA_0460 - Review account provisioning logs	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review user accounts</a>	CMA_0480 - Review user accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Service Fabric clusters should only use Azure Active Directory for client authentication</a>	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	<a href="#">1.1.0 ↗</a>

## Automated System Account Management

ID: NIST SP 800-53 Rev. 4 AC-2 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">An Azure Active Directory</a>	Audit provisioning of an Azure Active Directory administrator for your SQL server	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
administrator should be provisioned for SQL servers ↗	to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services		
Automate account management ↗	CMA_0026 - Automate account management	Manual, Disabled	1.1.0 ↗
Cognitive Services accounts should have local authentication methods disabled ↗	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> .	Audit, Deny, Disabled	1.0.0 ↗
Manage system and admin accounts ↗	CMA_0368 - Manage system and admin accounts	Manual, Disabled	1.1.0 ↗
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	1.1.0 ↗
Notify when account is not needed ↗	CMA_0383 - Notify when account is not needed	Manual, Disabled	1.1.0 ↗
Service Fabric clusters should only use Azure Active Directory for client authentication ↗	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	1.1.0 ↗

## Disable Inactive Accounts

ID: NIST SP 800-53 Rev. 4 AC-2 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	1.1.0 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗

## Automated Audit Actions

ID: NIST SP 800-53 Rev. 4 AC-2 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate account management ↗</a>	CMA_0026 - Automate account management	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage system and admin accounts ↗</a>	CMA_0368 - Manage system and admin accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Monitor access across the organization ↗</a>	CMA_0376 - Monitor access across the organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Notify when account is not needed ↗</a>	CMA_0383 - Notify when account is not needed	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Inactivity Logout

ID: NIST SP 800-53 Rev. 4 AC-2 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define and enforce inactivity log policy ↗</a>	CMA_C1017 - Define and enforce inactivity log policy	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Role-Based Schemes

ID: NIST SP 800-53 Rev. 4 AC-2 (7) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An Azure Active Directory administrator should be provisioned for SQL servers ↗	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	1.0.0 ↗
Audit privileged functions ↗	CMA_0019 - Audit privileged functions	Manual, Disabled	1.1.0 ↗
Audit usage of custom RBAC roles ↗	Audit built-in roles such as 'Owner', 'Contributer', 'Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling	Audit, Disabled	1.0.1 ↗
Cognitive Services accounts should have local authentication methods disabled ↗	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
Monitor account activity ↗	CMA_0377 - Monitor account activity	Manual, Disabled	1.1.0 ↗
Monitor privileged role assignment ↗	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	1.1.0 ↗
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	1.1.0 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗
Service Fabric clusters should only use Azure Active Directory for client authentication ↗	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	1.1.0 ↗
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↗

## Restrictions On Use Of Shared Groups / Accounts

ID: NIST SP 800-53 Rev. 4 AC-2 (9) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define and enforce conditions for shared and group accounts ↗</a>	CMA_0117 - Define and enforce conditions for shared and group accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Shared / Group Account Credential Termination

ID: NIST SP 800-53 Rev. 4 AC-2 (10) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Terminate customer controlled account credentials ↗</a>	CMA_C1022 - Terminate customer controlled account credentials	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Usage Conditions

ID: NIST SP 800-53 Rev. 4 AC-2 (11) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Enforce appropriate usage of all accounts ↗</a>	CMA_C1023 - Enforce appropriate usage of all accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Account Monitoring / Atypical Usage

ID: NIST SP 800-53 Rev. 4 AC-2 (12) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .	AuditIfNotExists, Disabled	6.0.0- preview ↗
Azure Defender for App Service should be enabled ↗	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Azure SQL Database servers should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for DNS should be enabled ↗	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for Key Vault should be enabled ↗	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Resource Manager	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
should be enabled ↗	about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for SQL servers on machines should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↗
Management ports of virtual machines should be protected with just-in-time network access control ↗	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.0.0 ↗
Microsoft Defender for Containers should be enabled ↗	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	1.0.0 ↗
Microsoft Defender for Storage	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
should be enabled ↗	workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.		
Monitor account activity ↗	CMA_0377 - Monitor account activity	Manual, Disabled	1.1.0 ↗
Report atypical behavior of user accounts ↗	CMA_C1025 - Report atypical behavior of user accounts	Manual, Disabled	1.1.0 ↗

## Disable Accounts For High-Risk Individuals

ID: NIST SP 800-53 Rev. 4 AC-2 (13) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Disable user accounts posing a significant risk ↗	CMA_C1026 - Disable user accounts posing a significant risk	Manual, Disabled	1.1.0 ↗

## Access Enforcement

ID: NIST SP 800-53 Rev. 4 AC-3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Accounts with owner permissions on Azure resources	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should be MFA enabled ↗</a>			
<a href="#">Accounts with read permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Accounts with write permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗ .	modify	<a href="#">4.0.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗ .	modify	<a href="#">4.0.0 ↗</a>
<a href="#">An Azure Active Directory administrator should be provisioned for SQL servers ↗</a>	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">App Service apps should use</a>	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name	Description	Effect(s)	Version
<a href="#">Audit Linux machines that have accounts without passwords</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if Linux machines that have accounts without passwords	AuditIfNotExists, Disabled	(GitHub) <a href="#">5.0.0</a>
<a href="#">Authentication to Linux machines should require SSH keys</a>	Although SSH itself provides an encrypted connection, using passwords with SSH still leaves the VM vulnerable to brute-force attacks. The most secure option for authenticating to an Azure Linux virtual machine over SSH is with a public-private key pair, also known as SSH keys. Learn more: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed">https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed</a> .	AuditIfNotExists, Disabled	<a href="#">3.1.0</a>
<a href="#">Authorize access to security functions and information</a>	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0</a>
<a href="#">Authorize and manage access</a>	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0</a>
<a href="#">Cognitive Services accounts should have local authentication methods disabled</a>	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> .	Audit, Deny, Disabled	<a href="#">1.0.0</a>
<a href="#">Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs</a>	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	<a href="#">3.0.0</a>
<a href="#">Enforce logical access</a>	CMA_0245 - Enforce logical access	Manual, Disabled	<a href="#">1.1.0</a>
<a href="#">Enforce mandatory and discretionary</a>	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
access control policies ↗			
Function apps should use managed identity ↗	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	3.0.0 ↗
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	1.1.0 ↗
Review user groups and applications with access to sensitive data ↗	CMA_0481 - Review user groups and applications with access to sensitive data	Manual, Disabled	1.1.0 ↗
Service Fabric clusters should only use Azure Active Directory for client authentication ↗	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	1.1.0 ↗
Storage accounts should be migrated to new Azure Resource Manager resources ↗	Use new Azure Resource Manager for your storage accounts to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management	Audit, Deny, Disabled	1.0.0 ↗
Virtual machines should be migrated to new Azure Resource Manager resources ↗	Use new Azure Resource Manager for your virtual machines to provide security enhancements such as: stronger access control (RBAC), better auditing, Azure Resource Manager based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management	Audit, Deny, Disabled	1.0.0 ↗

# Role-based Access Control

ID: NIST SP 800-53 Rev. 4 AC-3 (7) Ownership: Customer

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">Azure Role-Based Access Control (RBAC) should be used on Kubernetes Services ↗</a>	To provide granular filtering on the actions that users can perform, use Azure Role-Based Access Control (RBAC) to manage permissions in Kubernetes Service Clusters and configure relevant authorization policies.	Audit, Disabled	<a href="#">1.0.3 ↗</a>

# Information Flow Enforcement

ID: NIST SP 800-53 Rev. 4 AC-4 Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">[Preview]: All Internet traffic should be routed via your deployed Azure Firewall ↗</a>	Azure Security Center has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall	AuditIfNotExists, Disabled	<a href="#">3.0.0-preview ↗</a>
<a href="#">[Preview]: Storage account public access should be disallowed ↗</a>	Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing public access to a storage account unless your scenario requires it.	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">3.1.0-preview ↗</a>
<a href="#">Adaptive network hardening recommendations should be applied on internet facing virtual machines ↗</a>	Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
All network ports should be restricted on network security groups associated to your virtual machine ↗	Azure Security Center has identified some of your network security groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.	AuditIfNotExists, Disabled	3.0.0 ↗
API Management services should use a virtual network ↗	Azure Virtual Network deployment provides enhanced security, isolation and allows you to place your API Management service in a non-internet routable network that you control access to. These networks can then be connected to your on-premises networks using various VPN technologies, which enables access to your backend services within the network and/or on-premises. The developer portal and API gateway, can be configured to be accessible either from the Internet or only within the virtual network.	Audit, Deny, Disabled	1.0.2 ↗
App Configuration should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> ↗ .	AuditIfNotExists, Disabled	1.0.2 ↗
App Service apps should not have CORS configured to allow every resource to access your apps ↗	Cross-Origin Resource Sharing (CORS) should not allow all domains to access your app. Allow only required domains to interact with your app.	AuditIfNotExists, Disabled	2.0.0 ↗
Authorized IP ranges should be defined on	Restrict access to the Kubernetes Service Management API by granting API access only to IP addresses in specific ranges. It is recommended to limit access to authorized	Audit, Disabled	2.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Kubernetes Services ↗	IP ranges to ensure that only applications from allowed networks can access the cluster.		
Azure API for FHIR should use private link ↗	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> .	Audit, Disabled	1.0.0 ↗
Azure Cache for Redis should use private link ↗	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Cognitive Search service should use a SKU that supports private link ↗	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should disable public network access ↗	Disabling public network access improves security by ensuring that your Azure Cognitive Search service is not exposed on the public internet. Creating private endpoints can limit exposure of your Search service. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform	Audit, Disabled	1.0.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Azure Cognitive Search private link endpoint</a>	<p>Handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a>.</p>		
<a href="#">Azure Cosmos DB accounts should have firewall rules</a>	<p>Firewall rules should be defined on your Azure Cosmos DB accounts to prevent traffic from unauthorized sources.</p> <p>Accounts that have at least one IP rule defined with the virtual network filter enabled are deemed compliant. Accounts disabling public access are also deemed compliant.</p>	Audit, Deny, Disabled	2.0.0 <a href="#">↗</a>
<a href="#">Azure Data Factory should use private link</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a>.</p>	AuditIfNotExists, Disabled	1.0.0 <a href="#">↗</a>
<a href="#">Azure Event Grid domains should use private link</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a>.</p>	Audit, Disabled	1.0.2 <a href="#">↗</a>
<a href="#">Azure Event Grid topics should use private link</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure</p>	Audit, Disabled	1.0.2 <a href="#">↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a>.</p>		
Azure File Sync should use private link ↗	<p>Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.</p>	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Key Vault should have firewall enabled ↗	<p>Enable the key vault firewall so that the key vault is not accessible by default to any public IPs. Optionally, you can configure specific IP ranges to limit access to those networks. Learn more at: <a href="https://docs.microsoft.com/azure/key-vault/general/network-security">https://docs.microsoft.com/azure/key-vault/general/network-security</a></p>	Audit, Deny, Disabled	3.2.1 ↗
Azure Key Vaults should use private link ↗	<p>Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink</a>.</p>	[parameters('audit_effect')]	1.2.1 ↗
Azure Machine Learning workspaces should use private link ↗	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at:</p>	Audit, Disabled	1.0.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
	<a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .		
Azure Service Bus namespaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure SignalR Service should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .	Audit, Disabled	1.0.0 ↗
Azure Synapse workspaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a> .	Audit, Disabled	1.0.1 ↗
Azure Web PubSub Service should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Cognitive Services accounts should disable public network access ↗	<p>consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks.</p> <p>Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a>.</p>	Audit, Deny, Disabled	3.0.1 ↗
Cognitive Services accounts should restrict network access ↗	<p>To improve the security of Cognitive Services accounts, ensure that it isn't exposed to the public internet and can only be accessed from a private endpoint.</p> <p>Disable the public network access property as described in <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a>. This option disables access from any public address space outside the Azure IP range, and denies all logins that match IP or virtual network-based firewall rules. This reduces data leakage risks.</p>	Audit, Deny, Disabled	3.0.0 ↗
Cognitive Services should use private link ↗	<p>Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage.</p> <p>Learn more about private links at: <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a>.</p>	Audit, Disabled	3.0.0 ↗
Container registries should not allow	<p>Azure container registries by default accept connections over the internet from hosts on any network. To protect your registries</p>	Audit, Deny, Disabled	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
unrestricted network access ↗	from potential threats, allow access from only specific private endpoints, public IP addresses or address ranges. If your registry doesn't have network rules configured, it will appear in the unhealthy resources. Learn more about Container Registry network rules here: <a href="https://aka.ms/acr/privatelink">https://aka.ms/acr/privatelink</a> , ↗ <a href="https://aka.ms/acr/portal/public-network">https://aka.ms/acr/portal/public-network</a> ↗ and <a href="https://aka.ms/acr/vnet">https://aka.ms/acr/vnet</a> ↗ .		
Container registries should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a> ↗ .	Audit, Disabled	1.0.1 ↗
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	1.1.0 ↗
CosmosDB accounts should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a> .	Audit, Disabled	1.0.0 ↗
Disk access resources should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	risks are reduced. Learn more about private links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a> .		
Employ flow control mechanisms of encrypted information ↗	CMA_0211 - Employ flow control mechanisms of encrypted information	Manual, Disabled	1.1.0 ↗
Event Hub namespaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Internet-facing virtual machines should be protected with network security groups ↗	Protect your virtual machines from potential threats by restricting access to them with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsg-doc">https://aka.ms/nsg-doc</a>	AuditIfNotExists, Disabled	3.0.0 ↗
IoT Hub device provisioning service instances should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a> .	Audit, Disabled	1.0.0 ↗
IP Forwarding on your virtual machine should be disabled ↗	Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely required (e.g., when using the VM as a network virtual appliance), and therefore,	AuditIfNotExists, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	this should be reviewed by the network security team.		
Management ports of virtual machines should be protected with just-in-time network access control ↗	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.0.0 ↗
Management ports should be closed on your virtual machines ↗	Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine.	AuditIfNotExists, Disabled	3.0.0 ↗
Non-internet-facing virtual machines should be protected with network security groups ↗	Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsq-doc">https://aka.ms/nsq-doc</a> ↗	AuditIfNotExists, Disabled	3.0.0 ↗
Private endpoint connections on Azure SQL Database should be enabled ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↗
Private endpoint should be enabled for MariaDB servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for MySQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Private endpoint should be enabled for PostgreSQL servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↴
Public network access on Azure SQL Database should be disabled ↴	Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP or virtual network based firewall rules.	Audit, Deny, Disabled	1.1.0 ↴
Public network access should be disabled for MariaDB servers ↴	Disable the public network access property to improve security and ensure your Azure Database for MariaDB can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↴
Public network access should be disabled for MySQL servers ↴	Disable the public network access property to improve security and ensure your Azure Database for MySQL can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↴
Public network access should be disabled for PostgreSQL servers ↴	Disable the public network access property to improve security and ensure your Azure Database for PostgreSQL can only be accessed from a private endpoint. This configuration disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.1 ↴
Storage accounts should restrict network access ↴	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow	Audit, Deny, Disabled	1.1.1 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges		
<a href="#">Storage accounts should restrict network access using virtual network rules ↗</a>	Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.	Audit, Deny, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Storage accounts should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview ↗</a>	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Subnets should be associated with a Network Security Group ↗</a>	Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">VM Image Builder templates should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .	Audit, Disabled, Deny	<a href="#">1.1.0 ↗</a>

## Dynamic Information Flow Control

ID: NIST SP 800-53 Rev. 4 AC-4 (3) Ownership: Customer

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adaptive network hardening recommendations should be applied on internet facing virtual machines ↗	Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Management ports of virtual machines should be protected with just-in-time network access control ↗	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Security Policy Filters

ID: NIST SP 800-53 Rev. 4 AC-4 (8) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Information flow control using security policy filters ↗	CMA_C1029 - Information flow control using security policy filters	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Physical / Logical Separation Of Information Flows

ID: NIST SP 800-53 Rev. 4 AC-4 (21) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish firewall and router configuration standards ↗	CMA_0272 - Establish firewall and router configuration standards	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish network segmentation for card holder data environment ↗	CMA_0273 - Establish network segmentation for card holder data environment	Manual, Disabled	1.1.0 ↗
Identify and manage downstream information exchanges ↗	CMA_0298 - Identify and manage downstream information exchanges	Manual, Disabled	1.1.0 ↗

## Separation Of Duties

ID: NIST SP 800-53 Rev. 4 AC-5 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define access authorizations to support separation of duties ↗	CMA_0116 - Define access authorizations to support separation of duties	Manual, Disabled	1.1.0 ↗
Document separation of duties ↗	CMA_0204 - Document separation of duties	Manual, Disabled	1.1.0 ↗
Separate duties of individuals ↗	CMA_0492 - Separate duties of individuals	Manual, Disabled	1.1.0 ↗
There should be more than one owner assigned to your subscription ↗	It is recommended to designate more than one subscription owner in order to have administrator access redundancy.	AuditIfNotExists, Disabled	3.0.0 ↗

## Least Privilege

ID: NIST SP 800-53 Rev. 4 AC-6 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
A maximum of 3 owners should be	It is recommended to designate up to 3 subscription owners in order to reduce	AuditIfNotExists, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">designated for your subscription ↗</a>	the potential for breach by a compromised owner.		
<a href="#">Audit usage of custom RBAC roles ↗</a>	Audit built-in roles such as 'Owner, Contributer, Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Design an access control model ↗</a>	CMA_0129 - Design an access control model	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ least privilege access ↗</a>	CMA_0212 - Employ least privilege access	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Authorize Access To Security Functions

ID: NIST SP 800-53 Rev. 4 AC-6 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authorize access to security functions and information ↗</a>	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Authorize and manage access ↗</a>	CMA_0023 - Authorize and manage access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce mandatory and discretionary access control policies ↗</a>	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Privileged Accounts

ID: NIST SP 800-53 Rev. 4 AC-6 (5) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	1.1.0 ↗

## Review Of User Privileges

ID: NIST SP 800-53 Rev. 4 AC-6 (7) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
A maximum of 3 owners should be designated for your subscription ↗	It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.	AuditIfNotExists, Disabled	3.0.0 ↗
Audit usage of custom RBAC roles ↗	Audit built-in roles such as 'Owner', 'Contributer', 'Reader' instead of custom RBAC roles, which are error prone. Using custom roles is treated as an exception and requires a rigorous review and threat modeling	Audit, Disabled	1.0.1 ↗
Reassign or remove user privileges as needed ↗	CMA_C1040 - Reassign or remove user privileges as needed	Manual, Disabled	1.1.0 ↗
Review user privileges ↗	CMA_C1039 - Review user privileges	Manual, Disabled	1.1.0 ↗

## Privilege Levels For Code Execution

ID: NIST SP 800-53 Rev. 4 AC-6 (8) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce software execution privileges ↗	CMA_C1041 - Enforce software execution privileges	Manual, Disabled	1.1.0 ↗

# Auditing Use Of Privileged Functions

ID: NIST SP 800-53 Rev. 4 AC-6 (9) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit privileged functions ↗</a>	CMA_0019 - Audit privileged functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Conduct a full text analysis of logged privileged commands ↗</a>	CMA_0056 - Conduct a full text analysis of logged privileged commands	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Monitor privileged role assignment ↗</a>	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Restrict access to privileged accounts ↗</a>	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Revoke privileged roles as appropriate ↗</a>	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Use privileged identity management ↗</a>	CMA_0533 - Use privileged identity management	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Unsuccessful Logon Attempts

ID: NIST SP 800-53 Rev. 4 AC-7 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Enforce a limit of consecutive failed login attempts ↗</a>	CMA_C1044 - Enforce a limit of consecutive failed login attempts	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Concurrent Session Control

ID: NIST SP 800-53 Rev. 4 AC-10 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define and enforce the limit of concurrent sessions ↗	CMA_C1050 - Define and enforce the limit of concurrent sessions	Manual, Disabled	1.1.0 ↗

## Session Termination

ID: NIST SP 800-53 Rev. 4 AC-12 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Terminate user session automatically ↗	CMA_C1054 - Terminate user session automatically	Manual, Disabled	1.1.0 ↗

## User-Initiated Logouts / Message Displays

ID: NIST SP 800-53 Rev. 4 AC-12 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Display an explicit logout message ↗	CMA_C1056 - Display an explicit logout message	Manual, Disabled	1.1.0 ↗
Provide the logout capability ↗	CMA_C1055 - Provide the logout capability	Manual, Disabled	1.1.0 ↗

## Permitted Actions Without Identification Or Authentication

ID: NIST SP 800-53 Rev. 4 AC-14 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Identify actions allowed without authentication ↗	CMA_0295 - Identify actions allowed without authentication	Manual, Disabled	1.1.0 ↗

## Security Attributes

ID: NIST SP 800-53 Rev. 4 AC-16 Ownership: Customer

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	2.0.1 ↗
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↗

## Remote Access

ID: NIST SP 800-53 Rev. 4 AC-17 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	modify	4.0.0 ↗
Add system-assigned	This policy adds a system-assigned managed identity to virtual machines	modify	4.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↴	hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴.		
App Configuration should use private link ↴	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> ↴.	AuditIfNotExists, Disabled	1.0.2 ↴
App Service apps should have remote debugging turned off ↴	Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0 ↴
Audit Linux machines that allow remote connections from accounts without passwords ↴	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴. Machines are non-compliant if Linux machines that allow remote connections from accounts without passwords	AuditIfNotExists, Disabled	3.0.0 ↴
Authorize remote access ↴	CMA_0024 - Authorize remote access	Manual, Disabled	1.1.0 ↴
Azure API for FHIR should	Azure API for FHIR should have at least one approved private endpoint connection.	Audit, Disabled	1.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">use private link ↗</a>	Clients in a virtual network can securely access resources that have private endpoint connections through private links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> .		
<a href="#">Azure Cache for Redis should use private link ↗</a>	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Cognitive Search service should use a SKU that supports private link ↗</a>	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Cognitive Search services should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> .	Audit, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Data Factory should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a>.</p>		
<a href="#">Azure Event Grid domains should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a>.</p>	Audit, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Event Grid topics should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a>.</p>	Audit, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure File Sync should use private link ↗</a>	<p>Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.</p>	AuditIfExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Key Vaults should</a>	<p>Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or</p>	[parameters('audit_effect')]	<a href="#">1.2.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">use private link ↗</a>	destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink</a> .		
<a href="#">Azure Machine Learning workspaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .	Audit, Disabled	1.0.0 ↗
<a href="#">Azure Service Bus namespaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
<a href="#">Azure SignalR Service should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Spring Cloud should use network injection ↗	Azure Spring Cloud instances should use virtual network injection for the following purposes: 1. Isolate Azure Spring Cloud from Internet. 2. Enable Azure Spring Cloud to interact with systems in either on premises data centers or Azure service in other virtual networks. 3. Empower customers to control inbound and outbound network communications for Azure Spring Cloud.	Audit, Disabled, Deny	1.2.0 ↗
Azure Synapse workspaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a> .	Audit, Disabled	1.0.1 ↗
Azure Web PubSub Service should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a> ↗.	Audit, Disabled	1.0.0 ↗
Cognitive Services should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage. Learn more about private links at:	Audit, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> .		
Container registries should use private link ↳	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a> .	Audit, Disabled	1.0.1 ↳
CosmosDB accounts should use private link ↳	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a> .	Audit, Disabled	1.0.0 ↳
Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↳	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	3.0.0 ↳
Deploy the Windows Guest Configuration extension to enable Guest Configuration	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be	deployIfNotExists	1.2.0 ↳

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
assignments on Windows VMs ↗	deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .		
Disk access resources should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Document mobility training ↗	CMA_0191 - Document mobility training	Manual, Disabled	1.1.0 ↗
Document remote access guidelines ↗	CMA_0196 - Document remote access guidelines	Manual, Disabled	1.1.0 ↗
Event Hub namespaces should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Function apps should have remote debugging turned off ↗	Remote debugging requires inbound ports to be opened on Function apps. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0 ↗
Implement controls to secure	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
alternate work sites ↗			
IoT Hub device provisioning service instances should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a> ↗.	Audit, Disabled	1.0.0 ↗
Private endpoint connections on Azure SQL Database should be enabled ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↗
Private endpoint should be enabled for MariaDB servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for MySQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for PostgreSQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and	AuditIfNotExists, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	prevent access from all other IP addresses, including within Azure.		
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗
Storage accounts should restrict network access ↗	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges	Audit, Deny, Disabled	1.1.1 ↗
Storage accounts should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview</a> ↗	AuditIfNotExists, Disabled	2.0.0 ↗
VM Image Builder templates should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .	Audit, Disabled, Deny	1.1.0 ↗

## Automated Monitoring / Control

ID: NIST SP 800-53 Rev. 4 AC-17 (1) Ownership: Shared

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	4.0.0 ↗
Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	4.0.0 ↗
App Configuration should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> .	AuditIfNotExists, Disabled	1.0.2 ↗
App Service apps should have remote debugging turned off ↗	Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit Linux machines that allow remote connections from accounts without passwords ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Linux machines that allow remote connections from accounts without passwords	AuditIfNotExists, Disabled	3.0.0 ↗
Azure API for FHIR should use private link ↗	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> ↗.	Audit, Disabled	1.0.0 ↗
Azure Cache for Redis should use private link ↗	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Cognitive Search service should use a SKU that supports private link ↗	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.	Audit, Deny, Disabled	1.0.0 ↗
Azure Cognitive Search services should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints ↗</a> .		
Azure Data Factory should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Event Grid domains should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints ↗</a> .	Audit, Disabled	1.0.2 ↗
Azure Event Grid topics should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints ↗</a> .	Audit, Disabled	1.0.2 ↗
Azure File Sync should	Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">use private link ↗</a>	Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.		
<a href="#">Azure Key Vaults should use private link ↗</a>	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink</a> .	[parameters('audit_effect')]	<a href="#">1.2.1 ↗</a>
<a href="#">Azure Machine Learning workspaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .	Audit, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Service Bus namespaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure SignalR Service should</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or	Audit, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">use private link ↗</a>	destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .		
<a href="#">Azure Spring Cloud should use network injection ↗</a>	Azure Spring Cloud instances should use virtual network injection for the following purposes: 1. Isolate Azure Spring Cloud from Internet. 2. Enable Azure Spring Cloud to interact with systems in either on premises data centers or Azure service in other virtual networks. 3. Empower customers to control inbound and outbound network communications for Azure Spring Cloud.	Audit, Disabled, Deny	<a href="#">1.2.0 ↗</a>
<a href="#">Azure Synapse workspaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a> .	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Azure Web PubSub Service should use private link ↗</a>	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a> .	Audit, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Cognitive Services should use private link ↴	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage. Learn more about private links at: <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> .	Audit, Disabled	3.0.0 ↴
Container registries should use private link ↴	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a> .	Audit, Disabled	1.0.1 ↴
CosmosDB accounts should use private link ↴	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a> .	Audit, Disabled	1.0.0 ↴
Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↴	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition.	deployIfNotExists	3.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .		
Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	1.2.0
Disk access resources should use private link	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a> .	AuditIfNotExists, Disabled	1.0.0
Event Hub namespaces should use private link	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0
Function apps should have remote debugging turned off	Remote debugging requires inbound ports to be opened on Function apps. Remote debugging should be turned off.	AuditIfNotExists, Disabled	2.0.0
IoT Hub device provisioning	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or	Audit, Disabled	1.0.0

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
service instances should use private link ↗	destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a> ↗.		
Monitor access across the organization ↗	CMA_0376 - Monitor access across the organization	Manual, Disabled	1.1.0 ↗
Private endpoint connections on Azure SQL Database should be enabled ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↗
Private endpoint should be enabled for MariaDB servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for MySQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for PostgreSQL servers ↗	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and	AuditIfNotExists, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	prevent access from all other IP addresses, including within Azure.		
Storage accounts should restrict network access ↗	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges	Audit, Deny, Disabled	1.1.1 ↗
Storage accounts should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview</a> ↗	AuditIfNotExists, Disabled	2.0.0 ↗
VM Image Builder templates should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .	Audit, Disabled, Deny	1.1.0 ↗

## Protection Of Confidentiality / Integrity Using Encryption

ID: NIST SP 800-53 Rev. 4 AC-17 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Notify users of system logon or access ↗	CMA_0382 - Notify users of system logon or access	Manual, Disabled	1.1.0 ↗
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗

## Managed Access Control Points

ID: NIST SP 800-53 Rev. 4 AC-17 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	1.1.0 ↗

## Privileged Commands / Access

ID: NIST SP 800-53 Rev. 4 AC-17 (4) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize remote access ↗	CMA_0024 - Authorize remote access	Manual, Disabled	1.1.0 ↗
Authorize remote access to privileged commands ↗	CMA_C1064 - Authorize remote access to privileged commands	Manual, Disabled	1.1.0 ↗
Document remote access guidelines ↗	CMA_0196 - Document remote access guidelines	Manual, Disabled	1.1.0 ↗
Implement controls to secure alternate work sites ↗	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	1.1.0 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗

## Disconnect / Disable Access

ID: NIST SP 800-53 Rev. 4 AC-17 (9) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide capability to disconnect or disable remote access ↗	CMA_C1066 - Provide capability to disconnect or disable remote access	Manual, Disabled	1.1.0 ↗

## Wireless Access

ID: NIST SP 800-53 Rev. 4 AC-18 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document and implement wireless access guidelines ↗	CMA_0190 - Document and implement wireless access guidelines	Manual, Disabled	1.1.0 ↗
Protect wireless access ↗	CMA_0411 - Protect wireless access	Manual, Disabled	1.1.0 ↗

## Authentication And Encryption

ID: NIST SP 800-53 Rev. 4 AC-18 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document and implement wireless access guidelines ↗	CMA_0190 - Document and implement wireless access guidelines	Manual, Disabled	1.1.0 ↗
Identify and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	1.1.0 ↗
Protect wireless access ↗	CMA_0411 - Protect wireless access	Manual, Disabled	1.1.0 ↗

## Access Control For Mobile Devices

ID: NIST SP 800-53 Rev. 4 AC-19 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define mobile device requirements ↗</a>	CMA_0122 - Define mobile device requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Full Device / Container-Based Encryption

ID: NIST SP 800-53 Rev. 4 AC-19 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define mobile device requirements ↗</a>	CMA_0122 - Define mobile device requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Protect data in transit using encryption ↗</a>	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Use Of External Information Systems

ID: NIST SP 800-53 Rev. 4 AC-20 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish terms and conditions for accessing resources ↗</a>	CMA_C1076 - Establish terms and conditions for accessing resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish terms and conditions for processing resources ↗</a>	CMA_C1077 - Establish terms and conditions for processing resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Limits On Authorized Use

ID: NIST SP 800-53 Rev. 4 AC-20 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Verify security controls for external information systems ↗</a>	CMA_0541 - Verify security controls for external information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Portable Storage Devices

ID: NIST SP 800-53 Rev. 4 AC-20 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Block untrusted and unsigned processes that run from USB ↗</a>	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Control use of portable storage devices ↗</a>	CMA_0083 - Control use of portable storage devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information Sharing

ID: NIST SP 800-53 Rev. 4 AC-21 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Automate information sharing decisions ↗</a>	CMA_0028 - Automate information sharing decisions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Facilitate information sharing ↗</a>	CMA_0284 - Facilitate information sharing	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Publicly Accessible Content

ID: NIST SP 800-53 Rev. 4 AC-22 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Designate authorized personnel to post publicly accessible information ↗</a>	CMA_C1083 - Designate authorized personnel to post publicly accessible information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review content prior to posting publicly accessible information ↗</a>	CMA_C1085 - Review content prior to posting publicly accessible information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review publicly accessible content for nonpublic information ↗</a>	CMA_C1086 - Review publicly accessible content for nonpublic information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Train personnel on disclosure of nonpublic information ↗</a>	CMA_C1084 - Train personnel on disclosure of nonpublic information	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Awareness And Training

### Security Awareness And Training Policy Andprocedures

ID: NIST SP 800-53 Rev. 4 AT-1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Document security and privacy training activities ↗</a>	CMA_0198 - Document security and privacy training activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Update information security policies ↗</a>	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Awareness Training

ID: NIST SP 800-53 Rev. 4 AT-2 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide periodic security awareness training ↗	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 ↗
Provide security training for new users ↗	CMA_0419 - Provide security training for new users	Manual, Disabled	1.1.0 ↗
Provide updated security awareness training ↗	CMA_C1090 - Provide updated security awareness training	Manual, Disabled	1.1.0 ↗

## Insider Threat

ID: NIST SP 800-53 Rev. 4 AT-2 (2) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide security awareness training for insider threats ↗	CMA_0417 - Provide security awareness training for insider threats	Manual, Disabled	1.1.0 ↗

## Role-Based Security Training

ID: NIST SP 800-53 Rev. 4 AT-3 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide periodic role-based security training ↗	CMA_C1095 - Provide periodic role-based security training	Manual, Disabled	1.1.0 ↗
Provide role-based security training ↗	CMA_C1094 - Provide role-based security training	Manual, Disabled	1.1.0 ↗
Provide security training before providing access ↗	CMA_0418 - Provide security training before providing access	Manual, Disabled	1.1.0 ↗

## Practical Exercises

ID: NIST SP 800-53 Rev. 4 AT-3 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide role-based practical exercises ↗	CMA_C1096 - Provide role-based practical exercises	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Suspicious Communications And Anomalous System Behavior

ID: NIST SP 800-53 Rev. 4 AT-3 (4) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide role-based training on suspicious activities ↗	CMA_C1097 - Provide role-based training on suspicious activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Training Records

ID: NIST SP 800-53 Rev. 4 AT-4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor security and privacy training completion ↗	CMA_0379 - Monitor security and privacy training completion	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Retain training records ↗	CMA_0456 - Retain training records	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Audit And Accountability

### Audit And Accountability Policy And Procedures

ID: NIST SP 800-53 Rev. 4 AU-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop audit and accountability policies and procedures ↗	CMA_0154 - Develop audit and accountability policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Audit Events

ID: NIST SP 800-53 Rev. 4 AU-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Reviews And Updates

ID: NIST SP 800-53 Rev. 4 AU-2 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update the events defined in AU-02 ↗	CMA_C1106 - Review and update the events defined in AU-02	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Content Of Audit Records

ID: NIST SP 800-53 Rev. 4 AU-3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Determine auditable events ↗</a>	CMA_0137 - Determine auditable events	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Additional Audit Information

ID: NIST SP 800-53 Rev. 4 AU-3 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Configure Azure Audit capabilities ↗</a>	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	<a href="#">1.1.1 ↗</a>

## Audit Storage Capacity

ID: NIST SP 800-53 Rev. 4 AU-4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Govern and monitor audit processing activities ↗</a>	CMA_0289 - Govern and monitor audit processing activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Response To Audit Processing Failures

ID: NIST SP 800-53 Rev. 4 AU-5 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Govern and monitor audit processing activities ↗	CMA_0289 - Govern and monitor audit processing activities	Manual, Disabled	1.1.0 ↗

## Real-Time Alerts

ID: NIST SP 800-53 Rev. 4 AU-5 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide real-time alerts for audit event failures ↗	CMA_C1114 - Provide real-time alerts for audit event failures	Manual, Disabled	1.1.0 ↗

## Audit Review, Analysis, And Reporting

ID: NIST SP 800-53 Rev. 4 AU-6 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .	AuditIfNotExists, Disabled	6.0.0-preview ↗
[Preview]: Network traffic data collection agent should be installed on Linux	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
virtual machines ↗			
[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
Azure Defender for App Service should be enabled ↗	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Azure SQL Database servers should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for DNS should be enabled ↗	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for Key Vault should be enabled ↗	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Resource Manager	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
should be enabled ↗	about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for SQL servers on machines should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	2.0.1 ↗
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↗
Correlate audit records ↗	CMA_0087 - Correlate audit records	Manual, Disabled	1.1.0 ↗
Establish requirements for audit review and reporting ↗	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	1.1.0 ↗
Integrate audit review, ↗	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
analysis, and reporting ↗			
Integrate cloud app security with a siem ↗	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	1.1.0 ↗
Microsoft Defender for Containers should be enabled ↗	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	1.0.0 ↗
Microsoft Defender for Storage should be enabled ↗	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	1.0.0 ↗
Network Watcher should be enabled ↗	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	3.0.0 ↗
Review account provisioning logs ↗	CMA_0460 - Review account provisioning logs	Manual, Disabled	1.1.0 ↗
Review administrator assignments weekly ↗	CMA_0461 - Review administrator assignments weekly	Manual, Disabled	1.1.0 ↗
Review audit data ↗	CMA_0466 - Review audit data	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review cloud identity report overview ↗	CMA_0468 - Review cloud identity report overview	Manual, Disabled	1.1.0 ↗
Review controlled folder access events ↗	CMA_0471 - Review controlled folder access events	Manual, Disabled	1.1.0 ↗
Review file and folder activity ↗	CMA_0473 - Review file and folder activity	Manual, Disabled	1.1.0 ↗
Review role group changes weekly ↗	CMA_0476 - Review role group changes weekly	Manual, Disabled	1.1.0 ↗

## Process Integration

ID: NIST SP 800-53 Rev. 4 AU-6 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Correlate audit records ↗	CMA_0087 - Correlate audit records	Manual, Disabled	1.1.0 ↗
Establish requirements for audit review and reporting ↗	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	1.1.0 ↗
Integrate audit review, analysis, and reporting ↗	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	1.1.0 ↗
Integrate cloud app security with a siem ↗	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	1.1.0 ↗
Review account provisioning logs ↗	CMA_0460 - Review account provisioning logs	Manual, Disabled	1.1.0 ↗
Review administrator assignments weekly ↗	CMA_0461 - Review administrator assignments weekly	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review audit data ↗</a>	CMA_0466 - Review audit data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review cloud identity report overview ↗</a>	CMA_0468 - Review cloud identity report overview	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review controlled folder access events ↗</a>	CMA_0471 - Review controlled folder access events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review file and folder activity ↗</a>	CMA_0473 - Review file and folder activity	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review role group changes weekly ↗</a>	CMA_0476 - Review role group changes weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Correlate Audit Repositories

ID: NIST SP 800-53 Rev. 4 AU-6 (3) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Correlate audit records ↗</a>	CMA_0087 - Correlate audit records	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Integrate cloud app security with a siem ↗</a>	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Central Review And Analysis

ID: NIST SP 800-53 Rev. 4 AU-6 (4) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Preview]: Azure Arc enabled Kubernetes clusters should</a>	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes	AuditIfNotExists, Disabled	<a href="#">6.0.0-preview ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
have Microsoft Defender for Cloud extension installed ↗	backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .		
[Preview]: Log Analytics extension should be installed on your Linux Azure Arc machines ↗	This policy audits Linux Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1-preview ↗
[Preview]: Log Analytics extension should be installed on your Windows Azure Arc machines ↗	This policy audits Windows Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1-preview ↗
[Preview]: Network traffic data collection agent should be installed on Linux virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
App Service apps should have resource logs enabled ↗	Audit enabling of resource logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised.	AuditIfNotExists, Disabled	2.0.1 ↗
Auditing on SQL server	Auditing on your SQL Server should be enabled to track database activities across all databases	AuditIfNotExists, Disabled	2.0.0 ↗

Name should be enabled ↗ (Azure portal)	Description	Effect(s)	Version (GitHub)
Auto provisioning of the Log Analytics agent should be enabled on your subscription ↗	To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.	AuditIfNotExists, Disabled	1.0.1 ↗
Azure Defender for App Service should be enabled ↗	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Azure SQL Database servers should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for DNS should be enabled ↗	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for Key Vault should be enabled ↗	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Resource Manager	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
should be enabled ↗	about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
Azure Defender for SQL servers on machines should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Guest Configuration extension should be installed on your machines ↗	To ensure secure configurations of in-guest settings of your machine, install the Guest Configuration extension. In-guest settings that the extension monitors include the configuration of the operating system, application configuration or presence, and environment settings. Once installed, in-guest policies will be available such as 'Windows Exploit guard should be enabled'. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Log Analytics agent should be installed on your virtual machine for Azure Security Center monitoring ↴	This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring ↴	Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Microsoft Defender for Containers should be enabled ↴	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Microsoft Defender for Storage should be enabled ↴	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>
Network Watcher should be enabled ↴	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Resource logs in Azure Data Lake Store should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Azure Stream Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Batch accounts should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Data Lake Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Event Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in IoT Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
Resource logs in Key Vault should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Logic Apps should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.1.0 ↗</a>
Resource logs in Search	Audit enabling of resource logs. This enables you to recreate activity trails to use for	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">services should be enabled ↗</a>	investigation purposes; when a security incident occurs or when your network is compromised		
<a href="#">Resource logs in Service Bus should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity ↗</a>	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>

## Integration / Scanning And Monitoring Capabilities

ID: NIST SP 800-53 Rev. 4 AU-6 (5) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
<a href="#">[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗</a>	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .	AuditIfNotExists, Disabled	<a href="#">6.0.0-preview ↗</a>
<a href="#">[Preview]: Log Analytics extension should be installed on your Linux</a>	This policy audits Linux Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	<a href="#">1.0.1-preview ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Arc machines ↗			
[Preview]: Log Analytics extension should be installed on your Windows Azure Arc machines ↗	This policy audits Windows Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1-preview ↗
[Preview]: Network traffic data collection agent should be installed on Linux virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
App Service apps should have resource logs enabled ↗	Audit enabling of resource logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised.	AuditIfNotExists, Disabled	2.0.1 ↗
Auditing on SQL server should be enabled ↗	Auditing on your SQL Server should be enabled to track database activities across all databases on the server and save them in an audit log.	AuditIfNotExists, Disabled	2.0.0 ↗
Auto provisioning of the Log Analytics agent should be enabled on your subscription ↗	To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto	AuditIfNotExists, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.		
Azure Defender for App Service should be enabled ↗	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Azure SQL Database servers should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Azure Defender for DNS should be enabled ↗	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Defender for Key Vault should be enabled ↗	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	1.0.3 ↗
Azure Defender for Resource Manager should be enabled ↗	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for servers should be enabled ↴	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>
Azure Defender for SQL servers on machines should be enabled ↴	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↴	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↴</a>
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↴	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>
Guest Configuration extension should be installed on your machines ↴	To ensure secure configurations of in-guest settings of your machine, install the Guest Configuration extension. In-guest settings that the extension monitors include the configuration of the operating system, application configuration or presence, and environment settings. Once installed, in-guest policies will be available such as 'Windows Exploit guard should be enabled'. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>
Integrate Audit record analysis ↴	CMA_C1120 - Integrate Audit record analysis	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Log Analytics agent should be installed on your virtual machine for	This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Azure Security Center monitoring ↗</a>			
<a href="#">Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring ↗</a>	Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Containers should be enabled ↗</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Network Watcher should be enabled ↗</a>	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Resource logs in Azure Data Lake Store should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Resource logs in Azure Stream Analytics should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Resource logs in Batch accounts should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Resource logs in Data Lake Analytics should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Resource logs in Event Hub should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Resource logs in IoT Hub should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
<a href="#">Resource logs in Key Vault should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Resource logs in Logic Apps should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.1.0 ↗</a>
<a href="#">Resource logs in Search services should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Resource logs in Service Bus</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
should be enabled ↴	investigation purposes; when a security incident occurs or when your network is compromised		
Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity ↴	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴	AuditIfNotExists, Disabled	1.0.1 ↴

## Permitted Actions

ID: NIST SP 800-53 Rev. 4 AU-6 (7) Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Specify permitted actions associated with customer audit information ↴	CMA_C1122 - Specify permitted actions associated with customer audit information	Manual, Disabled	1.1.0 ↴

## Audit Level Adjustment

ID: NIST SP 800-53 Rev. 4 AU-6 (10) Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Adjust level of audit review, analysis, and reporting ↴	CMA_C1123 - Adjust level of audit review, analysis, and reporting	Manual, Disabled	1.1.0 ↴

## Audit Reduction And Report Generation

ID: NIST SP 800-53 Rev. 4 AU-7 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure audit records are not altered ↴	CMA_C1125 - Ensure audit records are not altered	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Provide audit review, analysis, and reporting capability ↴	CMA_C1124 - Provide audit review, analysis, and reporting capability	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Automatic Processing

ID: NIST SP 800-53 Rev. 4 AU-7 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide capability to process customer-controlled audit records ↴	CMA_C1126 - Provide capability to process customer-controlled audit records	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Time Stamps

ID: NIST SP 800-53 Rev. 4 AU-8 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Use system clocks for audit records ↴	CMA_0535 - Use system clocks for audit records	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Synchronization With Authoritative Time Source

ID: NIST SP 800-53 Rev. 4 AU-8 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Use system clocks for audit records ↗	CMA_0535 - Use system clocks for audit records	Manual, Disabled	1.1.0 ↗

## Protection Of Audit Information

ID: NIST SP 800-53 Rev. 4 AU-9 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enable dual or joint authorization ↗	CMA_0226 - Enable dual or joint authorization	Manual, Disabled	1.1.0 ↗
Protect audit information ↗	CMA_0401 - Protect audit information	Manual, Disabled	1.1.0 ↗

## Audit Backup On Separate Physical Systems / Components

ID: NIST SP 800-53 Rev. 4 AU-9 (2) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish backup policies and procedures ↗	CMA_0268 - Establish backup policies and procedures	Manual, Disabled	1.1.0 ↗

## Cryptographic Protection

ID: NIST SP 800-53 Rev. 4 AU-9 (3) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Maintain integrity of audit system ↗	CMA_C1133 - Maintain integrity of audit system	Manual, Disabled	1.1.0 ↗

## Access By Subset Of Privileged Users

ID: NIST SP 800-53 Rev. 4 AU-9 (4) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Protect audit information ↗	CMA_0401 - Protect audit information	Manual, Disabled	1.1.0 ↗

## Non-Repudiation

ID: NIST SP 800-53 Rev. 4 AU-10 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish electronic signature and certificate requirements ↗	CMA_0271 - Establish electronic signature and certificate requirements	Manual, Disabled	1.1.0 ↗

## Audit Record Retention

ID: NIST SP 800-53 Rev. 4 AU-11 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adhere to retention periods defined ↗	CMA_0004 - Adhere to retention periods defined	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Retain security policies and procedures ↗	CMA_0454 - Retain security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
SQL servers with auditing to storage account destination should be configured with 90 days retention or higher ↗	<p>For incident investigation purposes, we recommend setting the data retention for your SQL Server' auditing to storage account destination to at least 90 days.</p> <p>Confirm that you are meeting the necessary retention rules for the regions in which you are operating. This is sometimes required for compliance with regulatory standards.</p>	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Audit Generation

ID: NIST SP 800-53 Rev. 4 AU-12 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗	<p>Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a>.</p>	AuditIfNotExists, Disabled	<a href="#">6.0.0-preview ↗</a>
[Preview]: Log Analytics extension should be installed on your Linux Azure Arc machines ↗	This policy audits Linux Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	<a href="#">1.0.1-preview ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Log Analytics extension should be installed on your Windows Azure Arc machines ↗	This policy audits Windows Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1-preview ↗
[Preview]: Network traffic data collection agent should be installed on Linux virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
App Service apps should have resource logs enabled ↗	Audit enabling of resource logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised.	AuditIfNotExists, Disabled	2.0.1 ↗
Audit privileged functions ↗	CMA_0019 - Audit privileged functions	Manual, Disabled	1.1.0 ↗
Audit user account status ↗	CMA_0020 - Audit user account status	Manual, Disabled	1.1.0 ↗
Auditing on SQL server should be enabled ↗	Auditing on your SQL Server should be enabled to track database activities across all databases on the server and save them in an audit log.	AuditIfNotExists, Disabled	2.0.0 ↗
Auto provisioning of the Log Analytics agent should be	To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which	AuditIfNotExists, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">enabled on your subscription ↗</a>	reads various security-related configurations and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.		
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Resource Manager should be enabled ↗</a>	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for servers should be enabled ↗	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
Azure Defender for SQL servers on machines should be enabled ↗	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Guest Configuration extension should be installed on your machines ↗	To ensure secure configurations of in-guest settings of your machine, install the Guest Configuration extension. In-guest settings that the extension monitors include the configuration of the operating system, application configuration or presence, and environment settings. Once installed, in-guest policies will be available such as 'Windows Exploit guard should be enabled'. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Log Analytics agent should be installed on your virtual machine for Azure Security Center monitoring ↗</a>	This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring ↗</a>	Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Containers should be enabled ↗</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Network Watcher should be enabled ↗</a>	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Resource logs in Azure Data Lake Store should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Azure Stream Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Batch accounts should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Data Lake Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Event Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in IoT Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
Resource logs in Key Vault should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Logic Apps should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.1.0 ↗</a>
Resource logs in Search	Audit enabling of resource logs. This enables you to recreate activity trails to use for	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">services should be enabled ↗</a>	investigation purposes; when a security incident occurs or when your network is compromised		
<a href="#">Resource logs in Service Bus should be enabled ↗</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
<a href="#">Review audit data ↗</a>	CMA_0466 - Review audit data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity ↗</a>	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>

## System-Wide / Time-Correlated Audit Trail

ID: NIST SP 800-53 Rev. 4 AU-12 (1) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Preview]: Azure Arc enabled Kubernetes clusters should have Microsoft Defender for Cloud extension installed ↗</a>	Microsoft Defender for Cloud extension for Azure Arc provides threat protection for your Arc enabled Kubernetes clusters. The extension collects data from all nodes in the cluster and sends it to the Azure Defender for Kubernetes backend in the cloud for further analysis. Learn more in <a href="https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc">https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc</a> .	AuditIfNotExists, Disabled	<a href="#">6.0.0-preview ↗</a>
<a href="#">[Preview]: Log Analytics extension</a>	This policy audits Linux Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	<a href="#">1.0.1-preview ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
should be installed on your Linux Azure Arc machines ↗			
[Preview]: Log Analytics extension should be installed on your Windows Azure Arc machines ↗	This policy audits Windows Azure Arc machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1-preview ↗
[Preview]: Network traffic data collection agent should be installed on Linux virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
[Preview]: Network traffic data collection agent should be installed on Windows virtual machines ↗	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.	AuditIfNotExists, Disabled	1.0.2-preview ↗
App Service apps should have resource logs enabled ↗	Audit enabling of resource logs on the app. This enables you to recreate activity trails for investigation purposes if a security incident occurs or your network is compromised.	AuditIfNotExists, Disabled	2.0.1 ↗
Auditing on SQL server should be enabled ↗	Auditing on your SQL Server should be enabled to track database activities across all databases on the server and save them in an audit log.	AuditIfNotExists, Disabled	2.0.0 ↗
Auto provisioning of the Log Analytics agent should be enabled on	To monitor for security vulnerabilities and threats, Azure Security Center collects data from your Azure virtual machines. Data is collected by the Log Analytics agent, formerly known as the Microsoft Monitoring Agent (MMA), which reads various security-related configurations	AuditIfNotExists, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">your subscription ↗</a>	and event logs from the machine and copies the data to your Log Analytics workspace for analysis. We recommend enabling auto provisioning to automatically deploy the agent to all supported Azure VMs and any new ones that are created.		
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Resource Manager should be enabled ↗</a>	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> .		
Azure Defender for servers should be enabled ↴	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>
Azure Defender for SQL servers on machines should be enabled ↴	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↴	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↴</a>
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↴	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↴</a>
Compile Audit records into system wide audit ↴	CMA_C1140 - Compile Audit records into system wide audit	Manual, Disabled	<a href="#">1.1.0 ↴</a>
Guest Configuration extension should be installed on your machines ↴	To ensure secure configurations of in-guest settings of your machine, install the Guest Configuration extension. In-guest settings that the extension monitors include the configuration of the operating system, application configuration or presence, and environment settings. Once installed, in-guest policies will be available such as 'Windows Exploit guard should be enabled'. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↴</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Log Analytics agent should be installed on your virtual machine for Azure Security Center monitoring ↗</a>	This policy audits any Windows/Linux virtual machines (VMs) if the Log Analytics agent is not installed which Security Center uses to monitor for security vulnerabilities and threats	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Log Analytics agent should be installed on your virtual machine scale sets for Azure Security Center monitoring ↗</a>	Security Center collects data from your Azure virtual machines (VMs) to monitor for security vulnerabilities and threats.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Containers should be enabled ↗</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Network Watcher should be enabled ↗</a>	Network Watcher is a regional service that enables you to monitor and diagnose conditions at a network scenario level in, to, and from Azure. Scenario level monitoring enables you to diagnose problems at an end to end network level view. It is required to have a network watcher resource group to be created in every region where a virtual network is present. An alert is enabled if a network watcher resource group is not available in a particular region.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Resource logs in Azure Data Lake Store should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Azure Stream Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Batch accounts should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Data Lake Analytics should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Event Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in IoT Hub should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
Resource logs in Key Vault should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>
Resource logs in Logic Apps should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.1.0 ↗</a>
Resource logs in Search	Audit enabling of resource logs. This enables you to recreate activity trails to use for	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">services should be enabled ↴</a>	investigation purposes; when a security incident occurs or when your network is compromised		
<a href="#">Resource logs in Service Bus should be enabled ↴</a>	Audit enabling of resource logs. This enables you to recreate activity trails to use for investigation purposes; when a security incident occurs or when your network is compromised	AuditIfNotExists, Disabled	<a href="#">5.0.0 ↴</a>
<a href="#">Virtual machines' Guest Configuration extension should be deployed with system-assigned managed identity ↴</a>	The Guest Configuration extension requires a system assigned managed identity. Azure virtual machines in the scope of this policy will be non-compliant when they have the Guest Configuration extension installed but do not have a system assigned managed identity. Learn more at <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↴	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↴</a>

## Changes By Authorized Individuals

ID: NIST SP 800-53 Rev. 4 AU-12 (3) Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Provide the capability to extend or limit auditing on customer-deployed resources ↴</a>	CMA_C1141 - Provide the capability to extend or limit auditing on customer-deployed resources	Manual, Disabled	<a href="#">1.1.0 ↴</a>

## Security Assessment And Authorization

### Security Assessment And Authorization Policy And Procedures

ID: NIST SP 800-53 Rev. 4 CA-1 Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review security assessment and authorization policies and procedures ↗	CMA_C1143 - Review security assessment and authorization policies and procedures	Manual, Disabled	1.1.0 ↗

## Security Assessments

ID: NIST SP 800-53 Rev. 4 CA-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess Security Controls ↗	CMA_C1145 - Assess Security Controls	Manual, Disabled	1.1.0 ↗
Deliver security assessment results ↗	CMA_C1147 - Deliver security assessment results	Manual, Disabled	1.1.0 ↗
Develop security assessment plan ↗	CMA_C1144 - Develop security assessment plan	Manual, Disabled	1.1.0 ↗
Produce Security Assessment report ↗	CMA_C1146 - Produce Security Assessment report	Manual, Disabled	1.1.0 ↗

## Independent Assessors

ID: NIST SP 800-53 Rev. 4 CA-2 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ independent assessors to conduct security control assessments ↗	CMA_C1148 - Employ independent assessors to conduct security control assessments	Manual, Disabled	1.1.0 ↗

## Specialized Assessments

ID: NIST SP 800-53 Rev. 4 CA-2 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Select additional testing for security control assessments ↗	CMA_C1149 - Select additional testing for security control assessments	Manual, Disabled	1.1.0 ↗

## External Organizations

ID: NIST SP 800-53 Rev. 4 CA-2 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Accept assessment results ↗	CMA_C1150 - Accept assessment results	Manual, Disabled	1.1.0 ↗

## System Interconnections

ID: NIST SP 800-53 Rev. 4 CA-3 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require interconnection security agreements ↗	CMA_C1151 - Require interconnection security agreements	Manual, Disabled	1.1.0 ↗
Update interconnection security agreements ↗	CMA_0519 - Update interconnection security agreements	Manual, Disabled	1.1.0 ↗

## Unclassified Non-National Security System Connections

ID: NIST SP 800-53 Rev. 4 CA-3 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	1.1.0 ↗

## Restrictions On External System Connections

ID: NIST SP 800-53 Rev. 4 CA-3 (5) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ restrictions on external system interconnections ↗	CMA_C1155 - Employ restrictions on external system interconnections	Manual, Disabled	1.1.0 ↗

## Plan Of Action And Milestones

ID: NIST SP 800-53 Rev. 4 CA-5 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop POA&M ↗	CMA_C1156 - Develop POA&M	Manual, Disabled	1.1.0 ↗
Update POA&M items ↗	CMA_C1157 - Update POA&M items	Manual, Disabled	1.1.0 ↗

## Security Authorization

ID: NIST SP 800-53 Rev. 4 CA-6 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign an authorizing official (AO) ↗	CMA_C1158 - Assign an authorizing official (AO)	Manual, Disabled	1.1.0 ↗
Ensure resources are	CMA_C1159 - Ensure resources are	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">authorized ↗</a>	authorized	Disabled	
<a href="#">Update the security authorization ↗</a>	CMA_C1160 - Update the security authorization	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Continuous Monitoring

ID: NIST SP 800-53 Rev. 4 CA-7 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Configure detection whitelist ↗</a>	CMA_0068 - Configure detection whitelist	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Turn on sensors for endpoint security solution ↗</a>	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Undergo independent security review ↗</a>	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Independent Assessment

ID: NIST SP 800-53 Rev. 4 CA-7 (1) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ independent assessors for continuous monitoring ↗</a>	CMA_C1168 - Employ independent assessors for continuous monitoring	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Trend Analyses

ID: NIST SP 800-53 Rev. 4 CA-7 (3) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Analyse data obtained from continuous monitoring ↗	CMA_C1169 - Analyse data obtained from continuous monitoring	Manual, Disabled	1.1.0 ↗

## Independent Penetration Agent Or Team

ID: NIST SP 800-53 Rev. 4 CA-8 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ independent team for penetration testing ↗	CMA_C1171 - Employ independent team for penetration testing	Manual, Disabled	1.1.0 ↗

## Internal System Connections

ID: NIST SP 800-53 Rev. 4 CA-9 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Check for privacy and security compliance before establishing internal connections ↗	CMA_0053 - Check for privacy and security compliance before establishing internal connections	Manual, Disabled	1.1.0 ↗

## Configuration Management

### Configuration Management Policy And Procedures

ID: NIST SP 800-53 Rev. 4 CM-1 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update configuration management policies and procedures ↗	CMA_C1175 - Review and update configuration management policies and procedures	Manual, Disabled	1.1.0 ↗

## Baseline Configuration

ID: NIST SP 800-53 Rev. 4 CM-2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure actions for noncompliant devices ↗	CMA_0062 - Configure actions for noncompliant devices	Manual, Disabled	1.1.0 ↗
Develop and maintain baseline configurations ↗	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	1.1.0 ↗
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗
Establish a configuration control board ↗	CMA_0254 - Establish a configuration control board	Manual, Disabled	1.1.0 ↗
Establish and document a configuration management plan ↗	CMA_0264 - Establish and document a configuration management plan	Manual, Disabled	1.1.0 ↗
Implement an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	1.1.0 ↗

## Automation Support For Accuracy / Currency

ID: NIST SP 800-53 Rev. 4 CM-2 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure actions for	CMA_0062 - Configure actions for	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">noncompliant devices ↗</a>	noncompliant devices	Disabled	
<a href="#">Develop and maintain baseline configurations ↗</a>	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Enforce security configuration settings ↗</a>	CMA_0249 - Enforce security configuration settings	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a configuration control board ↗</a>	CMA_0254 - Establish a configuration control board	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and document a configuration management plan ↗</a>	CMA_0264 - Establish and document a configuration management plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement an automated configuration management tool ↗</a>	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Retention Of Previous Configurations

ID: NIST SP 800-53 Rev. 4 CM-2 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Retain previous versions of baseline configs ↗</a>	CMA_C1181 - Retain previous versions of baseline configs	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Configure Systems, Components, Or Devices For High-Risk Areas

ID: NIST SP 800-53 Rev. 4 CM-2 (7) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Ensure security safeguards not needed when the individuals</a>	CMA_C1183 - Ensure security safeguards not needed when the	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">return ↗</a>	individuals return		
<a href="#">Not allow for information systems to accompany with individuals ↗</a>	CMA_C1182 - Not allow for information systems to accompany with individuals	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Configuration Change Control

ID: NIST SP 800-53 Rev. 4 CM-3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Conduct a security impact analysis ↗</a>	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop and maintain a vulnerability management standard ↗</a>	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a risk management strategy ↗</a>	CMA_0258 - Establish a risk management strategy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and document change control processes ↗</a>	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish configuration management requirements for developers ↗</a>	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a privacy impact assessment ↗</a>	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a risk assessment ↗</a>	CMA_0388 - Perform a risk assessment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform audit for configuration change control ↗</a>	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Document / Notification / Prohibition Of Changes

ID: NIST SP 800-53 Rev. 4 CM-3 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Automate approval request for proposed changes ↗</a>	CMA_C1192 - Automate approval request for proposed changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate implementation of approved change notifications ↗</a>	CMA_C1196 - Automate implementation of approved change notifications	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate process to document implemented changes ↗</a>	CMA_C1195 - Automate process to document implemented changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate process to highlight unreviewed change proposals ↗</a>	CMA_C1193 - Automate process to highlight unreviewed change proposals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate process to prohibit implementation of unapproved changes ↗</a>	CMA_C1194 - Automate process to prohibit implementation of unapproved changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Automate proposed documented changes ↗</a>	CMA_C1191 - Automate proposed documented changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Test / Validate / Document Changes

ID: NIST SP 800-53 Rev. 4 CM-3 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish and document change control processes ↗</a>	CMA_0265 - Establish and document change control processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish configuration management requirements for developers ↗</a>	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform audit for configuration change control ↗</a>	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Representative

ID: NIST SP 800-53 Rev. 4 CM-3 (4) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign information security representative to change control ↗	CMA_C1198 - Assign information security representative to change control	Manual, Disabled	1.1.0 ↗

## Cryptography Management

ID: NIST SP 800-53 Rev. 4 CM-3 (6) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure cryptographic mechanisms are under configuration management ↗	CMA_C1199 - Ensure cryptographic mechanisms are under configuration management	Manual, Disabled	1.1.0 ↗

## Security Impact Analysis

ID: NIST SP 800-53 Rev. 4 CM-4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Develop and maintain a vulnerability management standard ↗	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	1.1.0 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for	CMA_0270 - Establish configuration management requirements for	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
developers ↗	developers		
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	1.1.0 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	1.1.0 ↗
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗

## Separate Test Environments

ID: NIST SP 800-53 Rev. 4 CM-4 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	1.1.0 ↗
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗

## Access Restrictions For Change

ID: NIST SP 800-53 Rev. 4 CM-5 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗

## Automated Access Enforcement / Auditing

ID: NIST SP 800-53 Rev. 4 CM-5 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce and audit access restrictions ↗	CMA_C1203 - Enforce and audit access restrictions	Manual, Disabled	1.1.0 ↗

## Review System Changes

ID: NIST SP 800-53 Rev. 4 CM-5 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review changes for any unauthorized changes ↗	CMA_C1204 - Review changes for any unauthorized changes	Manual, Disabled	1.1.0 ↗

## Signed Components

ID: NIST SP 800-53 Rev. 4 CM-5 (3) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Restrict unauthorized software and firmware installation ↗	CMA_C1205 - Restrict unauthorized software and firmware installation	Manual, Disabled	1.1.0 ↗

## Limit Production / Operational Privileges

ID: NIST SP 800-53 Rev. 4 CM-5 (5) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Limit privileges to make changes in production environment ↗</a>	CMA_C1206 - Limit privileges to make changes in production environment	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and reevaluate privileges ↗</a>	CMA_C1207 - Review and reevaluate privileges	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Configuration Settings

ID: NIST SP 800-53 Rev. 4 CM-6 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Deprecated]: Function apps should have 'Client Certificates (Incoming client certificates)' enabled ↗</a>	Client certificates allow for the app to request a certificate for incoming requests. Only clients with valid certificates will be able to reach the app. This policy has been replaced by a new policy with the same name because Http 2.0 doesn't support client certificates.	Audit, Disabled	<a href="#">3.1.0-deprecated ↗</a>
<a href="#">App Service apps should have Client Certificates (Incoming client certificates) enabled ↗</a>	Client certificates allow for the app to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the app. This policy applies to apps with Http version set to 1.1.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">App Service apps should have remote debugging turned off ↗</a>	Remote debugging requires inbound ports to be opened on an App Service app. Remote debugging should be turned off.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">App Service apps should not</a>	Cross-Origin Resource Sharing (CORS) should not allow all domains to access	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">have CORS configured to allow every resource to access your apps ↗</a>	your app. Allow only required domains to interact with your app.		
<a href="#">Azure Policy Add-on for Kubernetes service (AKS) should be installed and enabled on your clusters ↗</a>	Azure Policy Add-on for Kubernetes service (AKS) extends Gatekeeper v3, an admission controller webhook for Open Policy Agent (OPA), to apply at-scale enforcements and safeguards on your clusters in a centralized, consistent manner.	Audit, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Enforce security configuration settings ↗</a>	CMA_0249 - Enforce security configuration settings	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Function apps should have remote debugging turned off ↗</a>	Remote debugging requires inbound ports to be opened on Function apps. Remote debugging should be turned off.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Function apps should not have CORS configured to allow every resource to access your apps ↗</a>	Cross-Origin Resource Sharing (CORS) should not allow all domains to access your Function app. Allow only required domains to interact with your Function app.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Kubernetes cluster containers CPU and memory resource limits should not exceed the specified limits ↗</a>	Enforce container CPU and memory resource limits to prevent resource exhaustion attacks in a Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">9.1.0 ↗</a>
<a href="#">Kubernetes cluster containers should not</a>	Block pod containers from sharing the host process ID namespace and host IPC namespace in a Kubernetes cluster. This recommendation is part of CIS 5.2.2 and	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">5.1.0 ↗</a>

Name	Description	Effect(s)	Version
			(GitHub)
share host process ID or (Azure portal) host IPC namespace ↴	CIS 5.2.3 which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .		
Kubernetes cluster containers should only use allowed AppArmor profiles ↴	Containers should only use allowed AppArmor profiles in a Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.1 ↴
Kubernetes cluster containers should only use allowed capabilities ↴	Restrict the capabilities to reduce the attack surface of containers in a Kubernetes cluster. This recommendation is part of CIS 5.2.8 and CIS 5.2.9 which are intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.0 ↴
Kubernetes cluster containers should only use allowed images ↴	Use images from trusted registries to reduce the Kubernetes cluster's exposure risk to unknown vulnerabilities, security issues and malicious images. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	9.1.1 ↴
Kubernetes cluster containers should run with a read only root file system ↴	Run containers with a read only root file system to protect from changes at runtime with malicious binaries being added to PATH in a Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.0 ↴
Kubernetes cluster pod hostPath volumes should only use allowed host paths ↴	Limit pod HostPath volume mounts to the allowed host paths in a Kubernetes Cluster. This policy is generally available for Kubernetes Service (AKS), and Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.1 ↴

Name  (Azure portal)	Description	Effect(s)	Version  (GitHub)
<a href="#">Kubernetes cluster pods and containers should only run with approved user and group IDs ↗</a>	Control the user, primary group, supplemental group and file system group IDs that pods and containers can use to run in a Kubernetes Cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.1 ↗
<a href="#">Kubernetes cluster pods should only use approved host network and port range ↗</a>	Restrict pod access to the host network and the allowable host port range in a Kubernetes cluster. This recommendation is part of CIS 5.2.4 which is intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	6.1.0 ↗
<a href="#">Kubernetes cluster services should listen only on allowed ports ↗</a>	Restrict services to listen only on allowed ports to secure access to the Kubernetes cluster. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	8.1.0 ↗
<a href="#">Kubernetes cluster should not allow privileged containers ↗</a>	Do not allow privileged containers creation in a Kubernetes cluster. This recommendation is part of CIS 5.2.1 which is intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .	audit, Audit, deny, Deny, disabled, Disabled	9.1.0 ↗
<a href="#">Kubernetes clusters should not allow container privilege escalation ↗</a>	Do not allow containers to run with privilege escalation to root in a Kubernetes cluster. This recommendation is part of CIS 5.2.5 which is intended to improve the security of your Kubernetes environments. This policy is generally available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more	audit, Audit, deny, Deny, disabled, Disabled	7.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	information, see <a href="https://aka.ms/kubepolicydoc">https://aka.ms/kubepolicydoc</a> .		
Linux machines should meet requirements for the Azure compute security baseline ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if the machine is not configured correctly for one of the recommendations in the Azure compute security baseline.	AuditIfNotExists, Disabled	2.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗
Windows machines should meet requirements of the Azure compute security baseline ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-compliant if the machine is not configured correctly for one of the recommendations in the Azure compute security baseline.	AuditIfNotExists, Disabled	2.0.0 ↗

## Automated Central Management / Application / Verification

ID: NIST SP 800-53 Rev. 4 CM-6 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗
Govern compliance of cloud service providers ↗	CMA_0290 - Govern compliance of cloud service providers	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

## Least Functionality

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications should be enabled on your machines ↗</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Azure Defender for servers should be enabled ↗</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

## Prevent Program Execution

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should be enabled on your machines ↗</a>	rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.		
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Authorized Software / Whitelisting

ID: NIST SP 800-53 Rev. 4 CM-7 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications should be enabled on your machines ↗</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

# Information System Component Inventory

ID: NIST SP 800-53 Rev. 4 CM-8 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Create a data inventory ↗</a>	CMA_0096 - Create a data inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Maintain records of processing of personal data ↗</a>	CMA_0353 - Maintain records of processing of personal data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Updates During Installations / Removals

ID: NIST SP 800-53 Rev. 4 CM-8 (1) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Create a data inventory ↗</a>	CMA_0096 - Create a data inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Maintain records of processing of personal data ↗</a>	CMA_0353 - Maintain records of processing of personal data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Unauthorized Component Detection

ID: NIST SP 800-53 Rev. 4 CM-8 (3) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">Enable detection of network devices ↗</a>	CMA_0220 - Enable detection of network devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Set automated notifications for new and trending cloud applications in your organization ↗</a>	CMA_0495 - Set automated notifications for new and trending cloud applications in your organization	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Accountability Information

ID: NIST SP 800-53 Rev. 4 CM-8 (4) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Create a data inventory ↗</a>	CMA_0096 - Create a data inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and maintain an asset inventory ↗</a>	CMA_0266 - Establish and maintain an asset inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Configuration Management Plan

ID: NIST SP 800-53 Rev. 4 CM-9 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Create configuration plan protection ↗</a>	CMA_C1233 - Create configuration plan protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop and maintain baseline configurations ↗</a>	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop configuration item identification plan ↗</a>	CMA_C1231 - Develop configuration item identification plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop configuration management plan ↗</a>	CMA_C1232 - Develop configuration management plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and document a configuration management plan ↗</a>	CMA_0264 - Establish and document a configuration management plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement an automated configuration management tool ↗</a>	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Software Usage Restrictions

ID: NIST SP 800-53 Rev. 4 CM-10 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications should be enabled on your machines ↗</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Require compliance with intellectual property rights ↗</a>	CMA_0432 - Require compliance with intellectual property rights	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Track software license usage ↗</a>	CMA_C1235 - Track software license usage	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Open Source Software

ID: NIST SP 800-53 Rev. 4 CM-10 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Restrict use of open source software ↗</a>	CMA_C1237 - Restrict use of open source software	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## User-Installed Software

ID: NIST SP 800-53 Rev. 4 CM-11 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Adaptive application controls for defining safe applications should be enabled on your machines ↗</a>	Enable application controls to define the list of known-safe applications running on your machines, and alert you when other applications run. This helps harden your machines against malware. To simplify the process of configuring and maintaining your rules, Security Center uses machine learning to analyze the applications running on each machine and suggest the list of known-safe applications.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Allowlist rules in your adaptive application control policy should be updated ↗</a>	Monitor for changes in behavior on groups of machines configured for auditing by Azure Security Center's adaptive application controls. Security Center uses machine learning to analyze the running processes on your machines and suggest a list of known-safe applications. These are presented as recommended apps to allow in adaptive application control policies.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>

## Contingency Planning

### Contingency Planning Policy And Procedures

ID: NIST SP 800-53 Rev. 4 CP-1 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update contingency planning policies and procedures ↗</a>	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Contingency Plan

ID: NIST SP 800-53 Rev. 4 CP-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Communicate contingency plan changes ↗	CMA_C1249 - Communicate contingency plan changes	Manual, Disabled	1.1.0 ↗
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	1.1.0 ↗
Develop and document a business continuity and disaster recovery plan ↗	CMA_0146 - Develop and document a business continuity and disaster recovery plan	Manual, Disabled	1.1.0 ↗
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0 ↗
Develop contingency planning policies and procedures ↗	CMA_0156 - Develop contingency planning policies and procedures	Manual, Disabled	1.1.0 ↗
Distribute policies and procedures ↗	CMA_0185 - Distribute policies and procedures	Manual, Disabled	1.1.0 ↗
Review contingency plan ↗	CMA_C1247 - Review contingency plan	Manual, Disabled	1.1.0 ↗
Update contingency plan ↗	CMA_C1248 - Update contingency plan	Manual, Disabled	1.1.0 ↗

## Coordinate With Related Plans

ID: NIST SP 800-53 Rev. 4 CP-2 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	1.1.0 ↗

## Capacity Planning

ID: NIST SP 800-53 Rev. 4 CP-2 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct capacity planning ↗	CMA_C1252 - Conduct capacity planning	Manual, Disabled	1.1.0 ↗

## Resume Essential Missions / Business Functions

ID: NIST SP 800-53 Rev. 4 CP-2 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Plan for resumption of essential business functions ↗	CMA_C1253 - Plan for resumption of essential business functions	Manual, Disabled	1.1.0 ↗

## Resume All Missions / Business Functions

ID: NIST SP 800-53 Rev. 4 CP-2 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Resume all mission and business functions ↗	CMA_C1254 - Resume all mission and business functions	Manual, Disabled	1.1.0 ↗

## Continue Essential Missions / Business Functions

ID: NIST SP 800-53 Rev. 4 CP-2 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Plan for continuance of essential business functions ↗	CMA_C1255 - Plan for continuance of essential business functions	Manual, Disabled	1.1.0 ↗

## Identify Critical Assets

ID: NIST SP 800-53 Rev. 4 CP-2 (8) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">(Azure portal)</a>	CMA_0386 - Perform a business impact assessment and application criticality assessment ↗	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Contingency Training

ID: NIST SP 800-53 Rev. 4 CP-3 Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">(Azure portal)</a>	CMA_0412 - Provide contingency training ↗	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Simulated Events

ID: NIST SP 800-53 Rev. 4 CP-3 (1) Ownership: Shared

[\[+\] Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
<a href="#">(Azure portal)</a>	CMA_C1260 - Incorporate simulated contingency training ↗	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Contingency Plan Testing

ID: NIST SP 800-53 Rev. 4 CP-4 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Initiate contingency plan testing corrective actions ↗</a>	CMA_C1263 - Initiate contingency plan testing corrective actions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review the results of contingency plan testing ↗</a>	CMA_C1262 - Review the results of contingency plan testing	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Test the business continuity and disaster recovery plan ↗</a>	CMA_0509 - Test the business continuity and disaster recovery plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Coordinate With Related Plans

ID: NIST SP 800-53 Rev. 4 CP-4 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Coordinate contingency plans with related plans ↗</a>	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Alternate Processing Site

ID: NIST SP 800-53 Rev. 4 CP-4 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Evaluate alternate processing site capabilities ↗</a>	CMA_C1266 - Evaluate alternate processing site capabilities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Test contingency plan at an alternate processing location ↗</a>	CMA_C1265 - Test contingency plan at an alternate processing location	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Alternate Storage Site

ID: NIST SP 800-53 Rev. 4 CP-6 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Ensure alternate storage site safeguards are equivalent to primary site ↗</a>	CMA_C1268 - Ensure alternate storage site safeguards are equivalent to primary site	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish alternate storage site to store and retrieve backup information ↗</a>	CMA_C1267 - Establish alternate storage site to store and retrieve backup information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Geo-redundant backup should be enabled for Azure Database for MariaDB ↗</a>	Azure Database for MariaDB allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Geo-redundant backup should be enabled for Azure Database for MySQL ↗</a>	Azure Database for MySQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Geo-redundant backup should be enabled for Azure Database for PostgreSQL ↗</a>	Azure Database for PostgreSQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Geo-redundant storage should be</a>	Use geo-redundancy to create highly available applications	Audit, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">enabled for Storage Accounts ↗</a>			
<a href="#">Long-term geo-redundant backup should be enabled for Azure SQL Databases ↗</a>	This policy audits any Azure SQL Database with long-term geo-redundant backup not enabled.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

## Separation From Primary Site

ID: NIST SP 800-53 Rev. 4 CP-6 (1) Ownership: Shared

[+] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Create separate alternate and primary storage sites ↗</a>	CMA_C1269 - Create separate alternate and primary storage sites	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Geo-redundant backup should be enabled for Azure Database for MariaDB ↗</a>	Azure Database for MariaDB allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Geo-redundant backup should be enabled for Azure Database for MySQL ↗</a>	Azure Database for MySQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Geo-redundant backup should be enabled for Azure Database for PostgreSQL ↗</a>	Azure Database for PostgreSQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Geo-redundant storage should be enabled for Storage Accounts ↗</a>	Use geo-redundancy to create highly available applications	Audit, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Long-term geo-redundant backup should be enabled for Azure SQL Databases ↗</a>	This policy audits any Azure SQL Database with long-term geo-redundant backup not enabled.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

## Recovery Time / Point Objectives

ID: NIST SP 800-53 Rev. 4 CP-6 (2) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish alternate storage site that facilitates recovery operations ↗</a>	CMA_C1270 - Establish alternate storage site that facilitates recovery operations	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Accessibility

ID: NIST SP 800-53 Rev. 4 CP-6 (3) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Identify and mitigate potential issues at alternate storage site ↗	CMA_C1271 - Identify and mitigate potential issues at alternate storage site	Manual, Disabled	1.1.0 ↗

## Alternate Processing Site

ID: NIST SP 800-53 Rev. 4 CP-7 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit virtual machines without disaster recovery configured ↗	Audit virtual machines which do not have disaster recovery configured. To learn more about disaster recovery, visit <a href="https://aka.ms/asr-doc">https://aka.ms/asr-doc</a> ↗.	auditIfNotExists	1.0.0 ↗
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗

## Separation From Primary Site

ID: NIST SP 800-53 Rev. 4 CP-7 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗

## Accessibility

ID: NIST SP 800-53 Rev. 4 CP-7 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗

## Priority Of Service

ID: NIST SP 800-53 Rev. 4 CP-7 (3) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗
Establish requirements for internet service providers ↗	CMA_0278 - Establish requirements for internet service providers	Manual, Disabled	1.1.0 ↗

## Preparation For Use

ID: NIST SP 800-53 Rev. 4 CP-7 (4) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Prepare alternate processing site for use as operational site ↗	CMA_C1278 - Prepare alternate processing site for use as operational site	Manual, Disabled	1.1.0 ↗

## Priority Of Service Provisions

ID: NIST SP 800-53 Rev. 4 CP-8 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish requirements for internet service providers ↴	CMA_0278 - Establish requirements for internet service providers	Manual, Disabled	1.1.0 ↴

## Information System Backup

ID: NIST SP 800-53 Rev. 4 CP-9 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Backup should be enabled for Virtual Machines ↴	Ensure protection of your Azure Virtual Machines by enabling Azure Backup. Azure Backup is a secure and cost effective data protection solution for Azure.	AuditIfNotExists, Disabled	3.0.0 ↴
Conduct backup of information system documentation ↴	CMA_C1289 - Conduct backup of information system documentation	Manual, Disabled	1.1.0 ↴
Establish backup policies and procedures ↴	CMA_0268 - Establish backup policies and procedures	Manual, Disabled	1.1.0 ↴
Geo-redundant backup should be enabled for Azure Database for MariaDB ↴	Azure Database for MariaDB allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	1.0.1 ↴
Geo-redundant backup should be enabled for Azure Database for MySQL ↴	Azure Database for MySQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure.	Audit, Disabled	1.0.1 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Configuring geo-redundant storage for backup is only allowed during server create.		
<a href="#">Geo-redundant backup should be enabled for Azure Database for PostgreSQL ↗</a>	Azure Database for PostgreSQL allows you to choose the redundancy option for your database server. It can be set to a geo-redundant backup storage in which the data is not only stored within the region in which your server is hosted, but is also replicated to a paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.	Audit, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Key vaults should have deletion protection enabled ↗</a>	Malicious deletion of a key vault can lead to permanent data loss. You can prevent permanent data loss by enabling purge protection and soft delete. Purge protection protects you from insider attacks by enforcing a mandatory retention period for soft deleted key vaults. No one inside your organization or Microsoft will be able to purge your key vaults during the soft delete retention period. Keep in mind that key vaults created after September 1st 2019 have soft-delete enabled by default.	Audit, Deny, Disabled	<a href="#">2.1.0 ↗</a>
<a href="#">Key vaults should have soft delete enabled ↗</a>	Deleting a key vault without soft delete enabled permanently deletes all secrets, keys, and certificates stored in the key vault. Accidental deletion of a key vault can lead to permanent data loss. Soft delete allows you to recover an accidentally deleted key vault for a configurable retention period.	Audit, Deny, Disabled	<a href="#">3.0.0 ↗</a>

## Separate Storage For Critical Information

ID: NIST SP 800-53 Rev. 4 CP-9 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Separately store backup information ↗	CMA_C1293 - Separately store backup information	Manual, Disabled	1.1.0 ↗

## Transfer To Alternate Storage Site

ID: NIST SP 800-53 Rev. 4 CP-9 (5) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Transfer backup information to an alternate storage site ↗	CMA_C1294 - Transfer backup information to an alternate storage site	Manual, Disabled	1.1.0 ↗

## Information System Recovery And Reconstitution

ID: NIST SP 800-53 Rev. 4 CP-10 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Recover and reconstitute resources after any disruption ↗	CMA_C1295 - Recover and reconstitute resources after any disruption	Manual, Disabled	1.1.1 ↗

## Transaction Recovery

ID: NIST SP 800-53 Rev. 4 CP-10 (2) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement transaction based recovery ↗	CMA_C1296 - Implement transaction based recovery	Manual, Disabled	1.1.0 ↗

# Restore Within Time Period

ID: NIST SP 800-53 Rev. 4 CP-10 (4) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Restore resources to operational state ↗</a>	CMA_C1297 - Restore resources to operational state	Manual, Disabled	<a href="#">1.1.1 ↗</a>

# Identification And Authentication

## Identification And Authentication Policy And Procedures

ID: NIST SP 800-53 Rev. 4 IA-1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update identification and authentication policies and procedures ↗</a>	CMA_C1299 - Review and update identification and authentication policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Identification And Authentication (Organizational Users)

ID: NIST SP 800-53 Rev. 4 IA-2 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accounts with owner permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Accounts with read permissions on Azure</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">resources should be MFA enabled ↗</a>	with read privileges to prevent a breach of accounts or resources.		
<a href="#">Accounts with write permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">An Azure Active Directory administrator should be provisioned for SQL servers ↗</a>	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">App Service apps should use managed identity ↗</a>	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Cognitive Services accounts should have local authentication methods disabled ↗</a>	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> ↗ .	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Enforce user uniqueness ↗</a>	CMA_0250 - Enforce user uniqueness	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Function apps should use managed identity ↗</a>	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Service Fabric clusters should only use Azure Active Directory for client authentication ↗</a>	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Support personal verification credentials issued by legal authorities ↗</a>	CMA_0507 - Support personal verification credentials issued by legal authorities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Network Access To Privileged Accounts

ID: NIST SP 800-53 Rev. 4 IA-2 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accounts with owner permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Accounts with write permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Network Access To Non-Privileged Accounts

ID: NIST SP 800-53 Rev. 4 IA-2 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accounts with read permissions on Azure resources should be MFA enabled ↗</a>	Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Adopt biometric authentication mechanisms ↗</a>	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Local Access To Privileged Accounts

ID: NIST SP 800-53 Rev. 4 IA-2 (3) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adopt biometric authentication mechanisms ↗	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	1.1.0 ↗

## Group Authentication

ID: NIST SP 800-53 Rev. 4 IA-2 (5) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require use of individual authenticators ↗	CMA_C1305 - Require use of individual authenticators	Manual, Disabled	1.1.0 ↗

## Remote Access - Separate Device

ID: NIST SP 800-53 Rev. 4 IA-2 (11) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adopt biometric authentication mechanisms ↗	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	1.1.0 ↗
Identify and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	1.1.0 ↗

## Acceptance Of Piv Credentials

ID: NIST SP 800-53 Rev. 4 IA-2 (12) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Support personal verification credentials issued by legal	CMA_0507 - Support personal verification credentials issued by	Manual, Disabled	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">authorities ↗</a>	legal authorities		

## Identifier Management

ID: NIST SP 800-53 Rev. 4 IA-4 Ownership: Shared

[\[ \] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">An Azure Active Directory administrator should be provisioned for SQL servers ↗</a>	Audit provisioning of an Azure Active Directory administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">App Service apps should use managed identity ↗</a>	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Assign system identifiers ↗</a>	CMA_0018 - Assign system identifiers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Cognitive Services accounts should have local authentication methods disabled ↗</a>	Disabling local authentication methods improves security by ensuring that Cognitive Services accounts require Azure Active Directory identities exclusively for authentication. Learn more at: <a href="https://aka.ms/cs/auth">https://aka.ms/cs/auth</a> .	Audit, Deny, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Function apps should use managed identity ↗</a>	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Prevent identifier reuse for the defined time period ↗</a>	CMA_C1314 - Prevent identifier reuse for the defined time period	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Service Fabric clusters should only use Azure Active Directory for client authentication ↗</a>	Audit usage of client authentication only via Azure Active Directory in Service Fabric	Audit, Deny, Disabled	<a href="#">1.1.0 ↗</a>

# Identify User Status

ID: NIST SP 800-53 Rev. 4 IA-4 (4) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Identify status of individual users ↗</a>	CMA_C1316 - Identify status of individual users	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Authenticator Management

ID: NIST SP 800-53 Rev. 4 IA-5 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">[Preview]: Certificates should have the specified maximum validity period ↗</a>	Manage your organizational compliance requirements by specifying the maximum amount of time that a certificate can be valid within your key vault.	audit, Audit, deny, Deny, disabled, Disabled	<a href="#">2.2.0-preview ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	modify	<a href="#">4.0.0 ↗</a>
<a href="#">Add system-assigned managed identity to enable Guest Configuration assignments on</a>	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite	modify	<a href="#">4.0.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">VMs with a user-assigned identity ↗</a>	for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.		
<a href="#">Audit Linux machines that do not have the passwd file permissions set to 0644 ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Linux machines that do not have the passwd file permissions set to 0644	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Audit Windows machines that do not store passwords using reversible encryption ↗</a>	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Windows machines that do not store passwords using reversible encryption	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Authentication to Linux machines should require SSH keys ↗</a>	Although SSH itself provides an encrypted connection, using passwords with SSH still leaves the VM vulnerable to brute-force attacks. The most secure option for authenticating to an Azure Linux virtual machine over SSH is with a public-private key pair, also known as SSH keys. Learn more: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed">https://docs.microsoft.com/azure/virtual-machines/linux/create-ssh-keys-detailed</a> .	AuditIfNotExists, Disabled	<a href="#">3.1.0 ↗</a>
<a href="#">Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↗</a>	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.	deployIfNotExists	<a href="#">3.0.0 ↗</a>
<a href="#">Deploy the Windows Guest Configuration extension to enable Guest</a>	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a	deployIfNotExists	<a href="#">1.2.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Configuration assignments on Windows VMs ↗</a>	prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗.		
<a href="#">Establish authenticator types and processes ↗</a>	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish procedures for initial authenticator distribution ↗</a>	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement training for protecting authenticators ↗</a>	CMA_0329 - Implement training for protecting authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Key Vault keys should have an expiration date ↗</a>	Cryptographic keys should have a defined expiration date and not be permanent. Keys that are valid forever provide a potential attacker with more time to compromise the key. It is a recommended security practice to set expiration dates on cryptographic keys.	Audit, Deny, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Key Vault secrets should have an expiration date ↗</a>	Secrets should have a defined expiration date and not be permanent. Secrets that are valid forever provide a potential attacker with more time to compromise them. It is a recommended security practice to set expiration dates on secrets.	Audit, Deny, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Manage authenticator lifetime and reuse ↗</a>	CMA_0355 - Manage authenticator lifetime and reuse	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage Authenticators ↗</a>	CMA_C1321 - Manage Authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Refresh authenticators ↗</a>	CMA_0425 - Refresh authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Reissue authenticators for changed groups and accounts ↗	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	1.1.0 ↗
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	1.1.0 ↗

## Password-Based Authentication

ID: NIST SP 800-53 Rev. 4 IA-5 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Add system-assigned managed identity to enable Guest Configuration assignments on virtual machines with no identities ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration but do not have any managed identities. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	4.0.0 ↗
Add system-assigned managed identity to enable Guest Configuration assignments on VMs with a user-assigned identity ↗	This policy adds a system-assigned managed identity to virtual machines hosted in Azure that are supported by Guest Configuration and have at least one user-assigned identity but do not have a system-assigned managed identity. A system-assigned managed identity is a prerequisite for all Guest Configuration assignments and must be added to machines before using any Guest Configuration policy definitions. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	modify	4.0.0 ↗
Audit Linux machines that do not have the	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> . Machines are non-	AuditIfNotExists, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
passwd file permissions set to 0644 ↗	compliant if Linux machines that do not have the passwd file permissions set to 0644		
Audit Windows machines that allow re-use of the passwords after the specified number of unique passwords ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Windows machines that allow re-use of the passwords after the specified number of unique passwords. Default value for unique passwords is 24	AuditIfNotExists, Disabled	2.1.0 ↗
Audit Windows machines that do not have the maximum password age set to specified number of days ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Windows machines that do not have the maximum password age set to specified number of days. Default value for maximum password age is 70 days	AuditIfNotExists, Disabled	2.1.0 ↗
Audit Windows machines that do not have the minimum password age set to specified number of days ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Windows machines that do not have the minimum password age set to specified number of days. Default value for minimum password age is 1 day	AuditIfNotExists, Disabled	2.1.0 ↗
Audit Windows machines that do not have the password complexity setting enabled ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Windows machines that do not have the password complexity setting enabled	AuditIfNotExists, Disabled	2.0.0 ↗
Audit Windows machines that do not restrict the minimum password length to specified number of characters ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-compliant if Windows machines that do not restrict the minimum password length to specified number of characters. Default value for minimum password length is 14 characters	AuditIfNotExists, Disabled	2.1.0 ↗
Audit Windows machines that do not store passwords using	Requires that prerequisites are deployed to the policy assignment scope. For details, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> ↗. Machines are non-	AuditIfNotExists, Disabled	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
reversible encryption ↗	compliant if Windows machines that do not store passwords using reversible encryption		
Deploy the Linux Guest Configuration extension to enable Guest Configuration assignments on Linux VMs ↗	This policy deploys the Linux Guest Configuration extension to Linux virtual machines hosted in Azure that are supported by Guest Configuration. The Linux Guest Configuration extension is a prerequisite for all Linux Guest Configuration assignments and must be deployed to machines before using any Linux Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	3.0.0 ↗
Deploy the Windows Guest Configuration extension to enable Guest Configuration assignments on Windows VMs ↗	This policy deploys the Windows Guest Configuration extension to Windows virtual machines hosted in Azure that are supported by Guest Configuration. The Windows Guest Configuration extension is a prerequisite for all Windows Guest Configuration assignments and must be deployed to machines before using any Windows Guest Configuration policy definition. For more information on Guest Configuration, visit <a href="https://aka.ms/gcpol">https://aka.ms/gcpol</a> .	deployIfNotExists	1.2.0 ↗
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Establish a password policy ↗	CMA_0256 - Establish a password policy	Manual, Disabled	1.1.0 ↗
Implement parameters for memorized secret verifiers ↗	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	1.1.0 ↗
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	1.1.0 ↗

## Pki-Based Authentication

ID: NIST SP 800-53 Rev. 4 IA-5 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Bind authenticators and identities dynamically ↗	CMA_0035 - Bind authenticators and identities dynamically	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish authenticator types and processes ↗	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish parameters for searching secret authenticators and verifiers ↗	CMA_0274 - Establish parameters for searching secret authenticators and verifiers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish procedures for initial authenticator distribution ↗	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Map authenticated identities to individuals ↗	CMA_0372 - Map authenticated identities to individuals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Restrict access to private keys ↗	CMA_0445 - Restrict access to private keys	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## In-Person Or Trusted Third-Party Registration

ID: NIST SP 800-53 Rev. 4 IA-5 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Distribute authenticators ↗	CMA_0184 - Distribute authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Support For Password Strength Determination

ID: NIST SP 800-53 Rev. 4 IA-5 (4) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Establish a password policy ↗	CMA_0256 - Establish a password policy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement parameters for memorized secret verifiers ↗	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Protection Of Authenticators

ID: NIST SP 800-53 Rev. 4 IA-5 (6) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure authorized users protect provided authenticators ↗	CMA_C1339 - Ensure authorized users protect provided authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## No Embedded Unencrypted Static Authenticators

ID: NIST SP 800-53 Rev. 4 IA-5 (7) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure there are no unencrypted static authenticators ↗	CMA_C1340 - Ensure there are no unencrypted static authenticators	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Hardware Token-Based Authentication

ID: NIST SP 800-53 Rev. 4 IA-5 (11) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Satisfy token quality requirements ↗	CMA_0487 - Satisfy token quality requirements	Manual, Disabled	1.1.0 ↗

## Expiration Of Cached Authenticators

ID: NIST SP 800-53 Rev. 4 IA-5 (13) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce expiration of cached authenticators ↗	CMA_C1343 - Enforce expiration of cached authenticators	Manual, Disabled	1.1.0 ↗

## Authenticator Feedback

ID: NIST SP 800-53 Rev. 4 IA-6 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Obscure feedback information during authentication process ↗	CMA_C1344 - Obscure feedback information during authentication process	Manual, Disabled	1.1.0 ↗

## Cryptographic Module Authentication

ID: NIST SP 800-53 Rev. 4 IA-7 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authenticate to cryptographic module ↗	CMA_0021 - Authenticate to cryptographic module	Manual, Disabled	1.1.0 ↗

# Identification And Authentication (Non- Organizational Users)

ID: NIST SP 800-53 Rev. 4 IA-8 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Identify and authenticate non- organizational users ↗</a>	CMA_C1346 - Identify and authenticate non-organizational users	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Acceptance Of Piv Credentials From Other Agencies

ID: NIST SP 800-53 Rev. 4 IA-8 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accept PIV credentials ↗</a>	CMA_C1347 - Accept PIV credentials	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Acceptance Of Third-Party Credentials

ID: NIST SP 800-53 Rev. 4 IA-8 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Accept only FICAM-approved third-party credentials ↗</a>	CMA_C1348 - Accept only FICAM-approved third-party credentials	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Use Of Ficam-Approved Products

ID: NIST SP 800-53 Rev. 4 IA-8 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ FICAM-approved resources to accept third-party credentials ↗	CMA_C1349 - Employ FICAM-approved resources to accept third-party credentials	Manual, Disabled	1.1.0 ↗

## Use Of Ficam-Issued Profiles

ID: NIST SP 800-53 Rev. 4 IA-8 (4) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conform to FICAM-issued profiles ↗	CMA_C1350 - Conform to FICAM-issued profiles	Manual, Disabled	1.1.0 ↗

## Incident Response

### Incident Response Policy And Procedures

ID: NIST SP 800-53 Rev. 4 IR-1 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update incident response policies and procedures ↗	CMA_C1352 - Review and update incident response policies and procedures	Manual, Disabled	1.1.0 ↗

## Incident Response Training

ID: NIST SP 800-53 Rev. 4 IR-2 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗

## Simulated Events

ID: NIST SP 800-53 Rev. 4 IR-2 (1) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Incorporate simulated events into incident response training ↗	CMA_C1356 - Incorporate simulated events into incident response training	Manual, Disabled	1.1.0 ↗

## Automated Training Environments

ID: NIST SP 800-53 Rev. 4 IR-2 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ automated training environment ↗	CMA_C1357 - Employ automated training environment	Manual, Disabled	1.1.0 ↗

## Incident Response Testing

ID: NIST SP 800-53 Rev. 4 IR-3 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct incident response testing ↗	CMA_0060 - Conduct incident response testing	Manual, Disabled	1.1.0 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Run simulation attacks ↗</a>	CMA_0486 - Run simulation attacks	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Coordination With Related Plans

ID: NIST SP 800-53 Rev. 4 IR-3 (2) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Conduct incident response testing ↗</a>	CMA_0060 - Conduct incident response testing	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish an information security program ↗</a>	CMA_0263 - Establish an information security program	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Run simulation attacks ↗</a>	CMA_0486 - Run simulation attacks	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Incident Handling

ID: NIST SP 800-53 Rev. 4 IR-4 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess information security events ↗</a>	CMA_0013 - Assess information security events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should be enabled ↗</a>	that could indicate threats to SQL databases, and discovering and classifying sensitive data.		
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Resource Manager should be enabled ↗</a>	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for servers should be enabled ↗</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for SQL servers on machines should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for SQL should be enabled for</a>	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
unprotected Azure SQL servers ↗			
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↗
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Develop security safeguards ↗	CMA_0161 - Develop security safeguards	Manual, Disabled	1.1.0 ↗
Email notification for high severity alerts should be enabled ↗	To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, enable email notifications for high severity alerts in Security Center.	AuditIfNotExists, Disabled	1.0.1 ↗
Email notification to subscription owner for high severity alerts should be enabled ↗	To ensure your subscription owners are notified when there is a potential security breach in their subscription, set email notifications to subscription owners for high severity alerts in Security Center.	AuditIfNotExists, Disabled	2.0.0 ↗
Enable network protection ↗	CMA_0238 - Enable network protection	Manual, Disabled	1.1.0 ↗
Eradicate contaminated information ↗	CMA_0253 - Eradicate contaminated information	Manual, Disabled	1.1.0 ↗
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	1.1.0 ↗
Implement	CMA_0318 - Implement incident handling	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
incident handling ↗		Disabled	
Maintain incident response plan ↗	CMA_0352 - Maintain incident response plan	Manual, Disabled	1.1.0 ↗
Microsoft Defender for Containers should be enabled ↗	Microsoft Defender for Containers provides hardening, vulnerability assessment and runtime protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfExists, Disabled	1.0.0 ↗
Microsoft Defender for Storage should be enabled ↗	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfExists, Disabled	1.0.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Subscriptions should have a contact email address for security issues ↗	To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, set a security contact to receive email notifications from Security Center.	AuditIfExists, Disabled	1.0.1 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

## Automated Incident Handling Processes

ID: NIST SP 800-53 Rev. 4 IR-4 (1) Ownership: Shared

↗ Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Enable network protection ↗	CMA_0238 - Enable network protection	Manual, Disabled	1.1.0 ↗
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗

## Dynamic Reconfiguration

ID: NIST SP 800-53 Rev. 4 IR-4 (2) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Include dynamic reconfig of customer deployed resources ↗	CMA_C1364 - Include dynamic reconfig of customer deployed resources	Manual, Disabled	1.1.0 ↗

## Continuity Of Operations

ID: NIST SP 800-53 Rev. 4 IR-4 (3) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Identify classes of Incidents and Actions taken ↗	CMA_C1365 - Identify classes of Incidents and Actions taken	Manual, Disabled	1.1.0 ↗

## Information Correlation

ID: NIST SP 800-53 Rev. 4 IR-4 (4) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Insider Threats - Specific Capabilities

ID: NIST SP 800-53 Rev. 4 IR-4 (6) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement Incident handling capability ↗	CMA_C1367 - Implement Incident handling capability	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Correlation With External Organizations

ID: NIST SP 800-53 Rev. 4 IR-4 (8) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Coordinate with external organizations to achieve cross org perspective ↗	CMA_C1368 - Coordinate with external organizations to achieve cross org perspective	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Incident Monitoring

ID: NIST SP 800-53 Rev. 4 IR-5 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for App Service should be enabled ↗	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

Name (Azure portal)	Description	Effect(s) (GitHub)	Version
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Resource Manager should be enabled ↗</a>	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for servers should be enabled ↗</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for SQL servers on machines should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>

<b>Name</b>  (Azure portal)	<b>Description</b>	<b>Effect(s)</b>  (GitHub)	<b>Version</b>
<a href="#">Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↗</a>	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↗</a>
<a href="#">Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗</a>	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Email notification for high severity alerts should be enabled ↗</a>	To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, enable email notifications for high severity alerts in Security Center.	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Email notification to subscription owner for high severity alerts should be enabled ↗</a>	To ensure your subscription owners are notified when there is a potential security breach in their subscription, set email notifications to subscription owners for high severity alerts in Security Center.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Microsoft Defender for Containers should be enabled ↗</a>	Microsoft Defender for Containers provides hardening, vulnerability assessment and runtime protections for your Azure, hybrid, and multi-cloud Kubernetes environments.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Microsoft Defender for Storage should be enabled ↗</a>	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Subscriptions should have a</a>	To ensure the relevant people in your organization are notified when there is a	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">contact email address for security issues ↗</a>	potential security breach in one of your subscriptions, set a security contact to receive email notifications from Security Center.		

## Automated Reporting

ID: NIST SP 800-53 Rev. 4 IR-6 (1) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Document security operations ↗</a>	CMA_0202 - Document security operations	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Vulnerabilities Related to Incidents

ID: NIST SP 800-53 Rev. 4 IR-6 (2) Ownership: Customer

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Email notification for high severity alerts should be enabled ↗</a>	To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, enable email notifications for high severity alerts in Security Center.	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>
<a href="#">Email notification to subscription owner for high severity alerts should be enabled ↗</a>	To ensure your subscription owners are notified when there is a potential security breach in their subscription, set email notifications to subscription owners for high severity alerts in Security Center.	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>
<a href="#">Subscriptions should have a contact email address for security issues ↗</a>	To ensure the relevant people in your organization are notified when there is a potential security breach in one of your subscriptions, set a security contact to	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
receive email notifications from Security Center.			

## Incident Response Assistance

ID: NIST SP 800-53 Rev. 4 IR-7 Ownership: Shared

[\[+\]](#) Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Document security operations ↗	CMA_0202 - Document security operations	Manual, Disabled	1.1.0 ↗

## Automation Support For Availability Of Information / Support

ID: NIST SP 800-53 Rev. 4 IR-7 (1) Ownership: Shared

[\[+\]](#) Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Enable network protection ↗	CMA_0238 - Enable network protection	Manual, Disabled	1.1.0 ↗
Eradicate contaminated information ↗	CMA_0253 - Eradicate contaminated information	Manual, Disabled	1.1.0 ↗
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	1.1.0 ↗
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">View and investigate restricted users ↗</a>	CMA_0545 - View and investigate restricted users	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Coordination With External Providers

ID: NIST SP 800-53 Rev. 4 IR-7 (2) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Establish relationship between incident response capability and external providers ↗</a>	CMA_C1376 - Establish relationship between incident response capability and external providers	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Identify incident response personnel ↗</a>	CMA_0301 - Identify incident response personnel	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Incident Response Plan

ID: NIST SP 800-53 Rev. 4 IR-8 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess information security events ↗</a>	CMA_0013 - Assess information security events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Develop an incident response plan ↗</a>	CMA_0145 - Develop an incident response plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement incident handling ↗</a>	CMA_0318 - Implement incident handling	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Maintain data breach records ↗</a>	CMA_0351 - Maintain data breach records	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Maintain incident response plan ↗</a>	CMA_0352 - Maintain incident response plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Protect incident response plan ↗	CMA_0405 - Protect incident response plan	Manual, Disabled	1.1.0 ↗

## Information Spillage Response

ID: NIST SP 800-53 Rev. 4 IR-9 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Alert personnel of information spillage ↗	CMA_0007 - Alert personnel of information spillage	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Eradicate contaminated information ↗	CMA_0253 - Eradicate contaminated information	Manual, Disabled	1.1.0 ↗
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	1.1.0 ↗
Identify contaminated systems and components ↗	CMA_0300 - Identify contaminated systems and components	Manual, Disabled	1.1.0 ↗
Identify spilled information ↗	CMA_0303 - Identify spilled information	Manual, Disabled	1.1.0 ↗
Isolate information spills ↗	CMA_0346 - Isolate information spills	Manual, Disabled	1.1.0 ↗

## Responsible Personnel

ID: NIST SP 800-53 Rev. 4 IR-9 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Identify incident response personnel ↗	CMA_0301 - Identify incident response personnel	Manual, Disabled	1.1.0 ↗

# Training

ID: NIST SP 800-53 Rev. 4 IR-9 (2) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗

# Post-Spill Operations

ID: NIST SP 800-53 Rev. 4 IR-9 (3) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop spillage response procedures ↗	CMA_0162 - Develop spillage response procedures	Manual, Disabled	1.1.0 ↗

# Exposure To Unauthorized Personnel

ID: NIST SP 800-53 Rev. 4 IR-9 (4) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop security safeguards ↗	CMA_0161 - Develop security safeguards	Manual, Disabled	1.1.0 ↗

# Maintenance

## System Maintenance Policy And Procedures

ID: NIST SP 800-53 Rev. 4 MA-1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update system maintenance policies and procedures ↗</a>	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Controlled Maintenance

ID: NIST SP 800-53 Rev. 4 MA-2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ a media sanitization mechanism ↗</a>	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Maintenance Activities

ID: NIST SP 800-53 Rev. 4 MA-2 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Automate remote maintenance activities ↗</a>	CMA_C1402 - Automate remote maintenance activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Produce complete records of remote maintenance activities ↗</a>	CMA_C1403 - Produce complete records of remote maintenance activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Maintenance Tools

ID: NIST SP 800-53 Rev. 4 MA-3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Inspect Tools

ID: NIST SP 800-53 Rev. 4 MA-3 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Inspect Media

ID: NIST SP 800-53 Rev. 4 MA-3 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	activities		

## Prevent Unauthorized Removal

ID: NIST SP 800-53 Rev. 4 MA-3 (3) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control maintenance and repair activities ↗</a>	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Employ a media sanitization mechanism ↗</a>	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Nonlocal Maintenance

ID: NIST SP 800-53 Rev. 4 MA-4 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Document Nonlocal Maintenance

ID: NIST SP 800-53 Rev. 4 MA-4 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Manage nonlocal maintenance and diagnostic activities ↗</a>	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Comparable Security / Sanitization

ID: NIST SP 800-53 Rev. 4 MA-4 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Perform all non-local maintenance ↗</a>	CMA_C1417 - Perform all non-local maintenance	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Cryptographic Protection

ID: NIST SP 800-53 Rev. 4 MA-4 (6) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement cryptographic mechanisms ↗</a>	CMA_C1419 - Implement cryptographic mechanisms	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Maintenance Personnel

ID: NIST SP 800-53 Rev. 4 MA-5 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Designate personnel to supervise unauthorized maintenance</a>	CMA_C1422 - Designate personnel to supervise unauthorized	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
activities ↗	maintenance activities		
Maintain list of authorized remote maintenance personnel ↗	CMA_C1420 - Maintain list of authorized remote maintenance personnel	Manual, Disabled	1.1.0 ↗
Manage maintenance personnel ↗	CMA_C1421 - Manage maintenance personnel	Manual, Disabled	1.1.0 ↗

## Individuals Without Appropriate Access

ID: NIST SP 800-53 Rev. 4 MA-5 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗

## Timely Maintenance

ID: NIST SP 800-53 Rev. 4 MA-6 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide timely maintenance support ↗	CMA_C1425 - Provide timely maintenance support	Manual, Disabled	1.1.0 ↗

## Media Protection

### Media Protection Policy And Procedures

ID: NIST SP 800-53 Rev. 4 MP-1 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update media protection policies and procedures ↗</a>	CMA_C1427 - Review and update media protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Media Access

ID: NIST SP 800-53 Rev. 4 MP-2 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Media Marking

ID: NIST SP 800-53 Rev. 4 MP-3 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement controls to secure all media ↗</a>	CMA_0314 - Implement controls to secure all media	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Media Storage

ID: NIST SP 800-53 Rev. 4 MP-4 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ a media sanitization mechanism ↗</a>	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗

## Media Transport

ID: NIST SP 800-53 Rev. 4 MP-5 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗

## Cryptographic Protection

ID: NIST SP 800-53 Rev. 4 MP-5 (4) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗

## Media Sanitization

ID: NIST SP 800-53 Rev. 4 MP-6 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗

## Review / Approve / Track / Document / Verify

ID: NIST SP 800-53 Rev. 4 MP-6 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗

## Equipment Testing

ID: NIST SP 800-53 Rev. 4 MP-6 (2) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗

## Media Use

ID: NIST SP 800-53 Rev. 4 MP-7 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↗
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Restrict media use ↗	CMA_0450 - Restrict media use	Manual, Disabled	1.1.0 ↗

## Prohibit Use Without Owner

ID: NIST SP 800-53 Rev. 4 MP-7 (1) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Block untrusted and unsigned processes that run from USB ↗	CMA_0050 - Block untrusted and unsigned processes that run from USB	Manual, Disabled	1.1.0 ↗
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Restrict media use ↗	CMA_0450 - Restrict media use	Manual, Disabled	1.1.0 ↗

## Physical And Environmental Protection

### Physical And Environmental Protection Policy And Procedures

ID: NIST SP 800-53 Rev. 4 PE-1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update physical and environmental policies and procedures ↗</a>	CMA_C1446 - Review and update physical and environmental policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Physical Access Authorizations

ID: NIST SP 800-53 Rev. 4 PE-2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Physical Access Control

ID: NIST SP 800-53 Rev. 4 PE-3 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define a physical key management process ↗</a>	CMA_0115 - Define a physical key management process	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish and maintain an asset inventory ↗</a>	CMA_0266 - Establish and maintain an asset inventory	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Access Control For Transmission Medium

ID: NIST SP 800-53 Rev. 4 PE-4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Access Control For Output Devices

ID: NIST SP 800-53 Rev. 4 PE-5 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage the input, output, processing, and storage of data ↗</a>	CMA_0369 - Manage the input, output, processing, and storage of data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Intrusion Alarms / Surveillance Equipment

ID: NIST SP 800-53 Rev. 4 PE-6 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Install an alarm system ↗</a>	CMA_0338 - Install an alarm system	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage a secure surveillance camera system ↗</a>	CMA_0354 - Manage a secure surveillance camera system	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Visitor Access Records

ID: NIST SP 800-53 Rev. 4 PE-8 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Control physical access ↗</a>	CMA_0081 - Control physical access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Emergency Lighting

ID: NIST SP 800-53 Rev. 4 PE-12 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ automatic emergency lighting ↗</a>	CMA_0209 - Employ automatic emergency lighting	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Fire Protection

ID: NIST SP 800-53 Rev. 4 PE-13 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Detection Devices / Systems

ID: NIST SP 800-53 Rev. 4 PE-13 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement a penetration testing methodology ↗</a>	CMA_0306 - Implement a penetration testing methodology	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Run simulation attacks ↗</a>	CMA_0486 - Run simulation attacks	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Suppression Devices / Systems

ID: NIST SP 800-53 Rev. 4 PE-13 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automatic Fire Suppression

ID: NIST SP 800-53 Rev. 4 PE-13 (3) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Temperature And Humidity Controls

ID: NIST SP 800-53 Rev. 4 PE-14 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Monitoring With Alarms / Notifications

ID: NIST SP 800-53 Rev. 4 PE-14 (2) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Install an alarm system ↗</a>	CMA_0338 - Install an alarm system	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Water Damage Protection

ID: NIST SP 800-53 Rev. 4 PE-15 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement physical security for offices, working areas, and secure areas ↗</a>	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Delivery And Removal

ID: NIST SP 800-53 Rev. 4 PE-16 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define requirements for managing assets ↗	CMA_0125 - Define requirements for managing assets	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗

## Alternate Work Site

ID: NIST SP 800-53 Rev. 4 PE-17 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement controls to secure alternate work sites ↗	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	1.1.0 ↗

## Location Of Information System Components

ID: NIST SP 800-53 Rev. 4 PE-18 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement physical security for offices, working areas, and secure areas ↗	CMA_0323 - Implement physical security for offices, working areas, and secure areas	Manual, Disabled	1.1.0 ↗

## Planning

### Security Planning Policy And Procedures

ID: NIST SP 800-53 Rev. 4 PL-1 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update planning policies and procedures ↗	CMA_C1491 - Review and update planning policies and procedures	Manual, Disabled	1.1.0 ↗

## System Security Plan

ID: NIST SP 800-53 Rev. 4 PL-2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	1.1.0 ↗
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies and procedures	Manual, Disabled	1.1.0 ↗
Develop SSP that meets criteria ↗	CMA_C1492 - Develop SSP that meets criteria	Manual, Disabled	1.1.0 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	1.1.0 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗

## Plan / Coordinate With Other Organizational Entities

ID: NIST SP 800-53 Rev. 4 PL-2 (3) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish security requirements for the manufacturing of connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Rules Of Behavior

ID: NIST SP 800-53 Rev. 4 PL-4 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop acceptable use policies and procedures ↗	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce rules of behavior and access agreements ↗	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Social Media And Networking Restrictions

ID: NIST SP 800-53 Rev. 4 PL-4 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop acceptable use policies and procedures ↗</a>	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Information Security Architecture

ID: NIST SP 800-53 Rev. 4 PL-8 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Develop a concept of operations (CONOPS) ↗</a>	CMA_0141 - Develop a concept of operations (CONOPS)	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review and update the information security architecture ↗</a>	CMA_C1504 - Review and update the information security architecture	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Personnel Security

## Personnel Security Policy And Procedures

ID: NIST SP 800-53 Rev. 4 PS-1 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update personnel security policies and procedures ↗</a>	CMA_C1507 - Review and update personnel security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Position Risk Designation

ID: NIST SP 800-53 Rev. 4 PS-2 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assign risk designations ↗</a>	CMA_0016 - Assign risk designations	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Personnel Screening

ID: NIST SP 800-53 Rev. 4 PS-3 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Clear personnel with access to classified information ↗</a>	CMA_0054 - Clear personnel with access to classified information	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Implement personnel screening ↗</a>	CMA_0322 - Implement personnel screening	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Rescreen individuals at a defined frequency ↗</a>	CMA_C1512 - Rescreen individuals at a defined frequency	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information With Special Protection Measures

ID: NIST SP 800-53 Rev. 4 PS-3 (3) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Protect special information ↗</a>	CMA_0409 - Protect special information	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Personnel Termination

ID: NIST SP 800-53 Rev. 4 PS-4 Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct exit interview upon termination ↗	CMA_0058 - Conduct exit interview upon termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify upon termination or transfer ↗	CMA_0381 - Notify upon termination or transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Protect against and prevent data theft from departing employees ↗	CMA_0398 - Protect against and prevent data theft from departing employees	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Notification

ID: NIST SP 800-53 Rev. 4 PS-4 (2) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate notification of employee termination ↗	CMA_C1521 - Automate notification of employee termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Personnel Transfer

ID: NIST SP 800-53 Rev. 4 PS-5 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Initiate transfer or reassignment actions ↗	CMA_0333 - Initiate transfer or reassignment actions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Modify access authorizations upon personnel transfer ↗	CMA_0374 - Modify access authorizations upon personnel transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Notify upon termination or transfer ↗	CMA_0381 - Notify upon termination or transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Reevaluate access upon personnel transfer ↗	CMA_0424 - Reevaluate access upon personnel transfer	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Access Agreements

ID: NIST SP 800-53 Rev. 4 PS-6 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document organizational access agreements ↗	CMA_0192 - Document organizational access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Enforce rules of behavior and access agreements ↗	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Ensure access agreements are signed or resigned timely ↗	CMA_C1528 - Ensure access agreements are signed or resigned timely	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require users to sign access agreement ↗	CMA_0440 - Require users to sign access agreement	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Update organizational access agreements ↗	CMA_0520 - Update organizational access agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Third-Party Personnel Security

ID: NIST SP 800-53 Rev. 4 PS-7 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document third-party personnel security requirements ↗	CMA_C1531 - Document third-party personnel security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require notification of third-party personnel transfer or termination ↗	CMA_C1532 - Require notification of third-party personnel transfer or termination	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require third-party providers to comply with personnel security policies and procedures ↗	CMA_C1530 - Require third-party providers to comply with personnel security policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Personnel Sanctions

ID: NIST SP 800-53 Rev. 4 PS-8 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement formal sanctions process ↗	CMA_0317 - Implement formal sanctions process	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Notify personnel upon sanctions ↗	CMA_0380 - Notify personnel upon sanctions	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Risk Assessment

### Risk Assessment Policy And Procedures

ID: NIST SP 800-53 Rev. 4 RA-1 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update risk assessment policies and	CMA_C1537 - Review and update risk assessment policies and	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
procedures ↗	procedures		

## Security Categorization

ID: NIST SP 800-53 Rev. 4 RA-2 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Categorize information ↗	CMA_0052 - Categorize information	Manual, Disabled	1.1.0 ↗
Develop business classification schemes ↗	CMA_0155 - Develop business classification schemes	Manual, Disabled	1.1.0 ↗
Ensure security categorization is approved ↗	CMA_C1540 - Ensure security categorization is approved	Manual, Disabled	1.1.0 ↗
Review label activity and analytics ↗	CMA_0474 - Review label activity and analytics	Manual, Disabled	1.1.0 ↗

## Risk Assessment

ID: NIST SP 800-53 Rev. 4 RA-3 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct Risk Assessment ↗	CMA_C1543 - Conduct Risk Assessment	Manual, Disabled	1.1.0 ↗
Conduct risk assessment and distribute its results ↗	CMA_C1544 - Conduct risk assessment and distribute its results	Manual, Disabled	1.1.0 ↗
Conduct risk assessment and document its results ↗	CMA_C1542 - Conduct risk assessment and document its results	Manual, Disabled	1.1.0 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	1.1.0 ↗

# Vulnerability Scanning

ID: NIST SP 800-53 Rev. 4 RA-5 Ownership: Shared

 Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">A vulnerability assessment solution should be enabled on your virtual machines ↗</a>	Audits virtual machines to detect whether they are running a supported vulnerability assessment solution. A core component of every cyber risk and security program is the identification and analysis of vulnerabilities. Azure Security Center's standard pricing tier includes vulnerability scanning for your virtual machines at no extra cost. Additionally, Security Center can automatically deploy this tool for you.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Azure Defender for App Service should be enabled ↗</a>	Azure Defender for App Service leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Azure Defender for Azure SQL Database servers should be enabled ↗</a>	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Azure Defender for DNS should be enabled ↗</a>	Azure Defender for DNS provides an additional layer of protection for your cloud resources by continuously monitoring all DNS queries from your Azure resources. Azure Defender alerts you about suspicious activity at the DNS layer. Learn more about the capabilities of Azure Defender for DNS at <a href="https://aka.ms/defender-for-dns">https://aka.ms/defender-for-dns</a> ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↗ .	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>
<a href="#">Azure Defender for Key Vault should be enabled ↗</a>	Azure Defender for Key Vault provides an additional layer of protection and security intelligence by detecting unusual and potentially harmful attempts to access or exploit key vault accounts.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for Resource Manager should be enabled ↴	Azure Defender for Resource Manager automatically monitors the resource management operations in your organization. Azure Defender detects threats and alerts you about suspicious activity. Learn more about the capabilities of Azure Defender for Resource Manager at <a href="https://aka.ms/defender-for-resource-manager">https://aka.ms/defender-for-resource-manager</a> ↴ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: <a href="https://aka.ms/pricing-security-center">https://aka.ms/pricing-security-center</a> ↴ .	AuditIfNotExists, Disabled	1.0.0 ↴
Azure Defender for servers should be enabled ↴	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	1.0.3 ↴
Azure Defender for SQL servers on machines should be enabled ↴	Azure Defender for SQL provides functionality for surfacing and mitigating potential database vulnerabilities, detecting anomalous activities that could indicate threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↴
Azure Defender for SQL should be enabled for unprotected Azure SQL servers ↴	Audit SQL servers without Advanced Data Security	AuditIfNotExists, Disabled	2.0.1 ↴
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↴	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↴
Container registry images should have vulnerability findings resolved ↴	Container image vulnerability assessment scans your registry for security vulnerabilities and exposes detailed findings for each image. Resolving the vulnerabilities can greatly improve your containers' security posture and protect them from attacks.	AuditIfNotExists, Disabled	2.0.1 ↴
Microsoft Defender for	Microsoft Defender for Containers provides hardening, vulnerability assessment and run-	AuditIfNotExists, Disabled	1.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Containers should be enabled ↗	time protections for your Azure, hybrid, and multi-cloud Kubernetes environments.		
Microsoft Defender for Storage should be enabled ↗	Microsoft Defender for Storage detects potential threats to your storage accounts. It helps prevent the three major impacts on your data and workload: malicious file uploads, sensitive data exfiltration, and data corruption. The new Defender for Storage plan includes Malware Scanning and Sensitive Data Threat Detection. This plan also provides a predictable pricing structure (per storage account) for control over coverage and costs.	AuditIfNotExists, Disabled	1.0.0 ↗
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗
SQL databases should have vulnerability findings resolved ↗	Monitor vulnerability assessment scan results and recommendations for how to remediate database vulnerabilities.	AuditIfNotExists, Disabled	4.1.0 ↗
SQL servers on machines should have vulnerability findings resolved ↗	SQL vulnerability assessment scans your database for security vulnerabilities, and exposes any deviations from best practices such as misconfigurations, excessive permissions, and unprotected sensitive data. Resolving the vulnerabilities found can greatly improve your database security posture.	AuditIfNotExists, Disabled	1.0.0 ↗
Vulnerabilities in container security configurations should be remediated ↗	Audit vulnerabilities in security configuration on machines with Docker installed and display as recommendations in Azure Security Center.	AuditIfNotExists, Disabled	3.0.0 ↗
Vulnerabilities in security configuration on your machines should be remediated ↗	Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	3.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Vulnerabilities in security configuration on your virtual machine scale sets should be remediated ↗	Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Vulnerability assessment should be enabled on SQL Managed Instance ↗	Audit each SQL Managed Instance which doesn't have recurring vulnerability assessment scans enabled. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">1.0.1 ↗</a>
Vulnerability assessment should be enabled on your SQL servers ↗	Audit Azure SQL servers which do not have vulnerability assessment properly configured. Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
Vulnerability assessment should be enabled on your Synapse workspaces ↗	Discover, track, and remediate potential vulnerabilities by configuring recurring SQL vulnerability assessment scans on your Synapse workspaces.	AuditIfNotExists, Disabled	<a href="#">1.0.0 ↗</a>

## Update Tool Capability

ID: NIST SP 800-53 Rev. 4 RA-5 (1) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform vulnerability scans ↗	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Update By Frequency / Prior To New Scan / When Identified

ID: NIST SP 800-53 Rev. 4 RA-5 (2) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Perform vulnerability scans ↗</a>	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Breadth / Depth Of Coverage

ID: NIST SP 800-53 Rev. 4 RA-5 (3) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Perform vulnerability scans ↗</a>	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Discoverable Information

ID: NIST SP 800-53 Rev. 4 RA-5 (4) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Take action in response to customer information ↗</a>	CMA_C1554 - Take action in response to customer information	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Privileged Access

ID: NIST SP 800-53 Rev. 4 RA-5 (5) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement privileged access for executing vulnerability scanning activities ↗</a>	CMA_C1555 - Implement privileged access for executing vulnerability scanning activities	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Automated Trend Analyses

ID: NIST SP 800-53 Rev. 4 RA-5 (6) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Observe and report security weaknesses ↗</a>	CMA_0384 - Observe and report security weaknesses	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform a trend analysis on threats ↗</a>	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform threat modeling ↗</a>	CMA_0392 - Perform threat modeling	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Perform vulnerability scans ↗</a>	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Review Historic Audit Logs

ID: NIST SP 800-53 Rev. 4 RA-5 (8) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit privileged functions ↗</a>	CMA_0019 - Audit privileged functions	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Audit user account status ↗</a>	CMA_0020 - Audit user account status	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Correlate audit records ↗</a>	CMA_0087 - Correlate audit records	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Determine auditable events ↗</a>	CMA_0137 - Determine auditable events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish requirements for audit review and reporting ↗</a>	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Integrate audit review, analysis, and reporting ↗</a>	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Integrate cloud app security with a siem ↗</a>	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review account provisioning logs ↗</a>	CMA_0460 - Review account provisioning logs	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review administrator assignments weekly ↗</a>	CMA_0461 - Review administrator assignments weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review audit data ↗</a>	CMA_0466 - Review audit data	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review cloud identity report overview ↗</a>	CMA_0468 - Review cloud identity report overview	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review controlled folder access events ↗</a>	CMA_0471 - Review controlled folder access events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review exploit protection events ↗</a>	CMA_0472 - Review exploit protection events	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review file and folder activity ↗</a>	CMA_0473 - Review file and folder activity	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Review role group changes weekly ↗</a>	CMA_0476 - Review role group changes weekly	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Correlate Scanning Information

ID: NIST SP 800-53 Rev. 4 RA-5 (10) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Correlate Vulnerability scan information ↗</a>	CMA_C1558 - Correlate Vulnerability scan information	Manual, Disabled	<a href="#">1.1.1 ↗</a>

## System And Services Acquisition

### System And Services Acquisition Policy And Procedures

ID: NIST SP 800-53 Rev. 4 SA-1 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review and update system and services acquisition policies and procedures ↗</a>	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Allocation Of Resources

ID: NIST SP 800-53 Rev. 4 SA-2 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Align business objectives and IT goals ↗</a>	CMA_0008 - Align business objectives and IT goals	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Allocate resources in determining information system requirements ↗</a>	CMA_C1561 - Allocate resources in determining information system requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a discrete line item in budgeting documentation ↗</a>	CMA_C1563 - Establish a discrete line item in budgeting documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish a privacy program ↗</a>	CMA_0257 - Establish a privacy program	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Govern the allocation of resources ↗	CMA_0293 - Govern the allocation of resources	Manual, Disabled	1.1.0 ↗
Secure commitment from leadership ↗	CMA_0489 - Secure commitment from leadership	Manual, Disabled	1.1.0 ↗

## System Development Life Cycle

ID: NIST SP 800-53 Rev. 4 SA-3 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define information security roles and responsibilities ↗	CMA_C1565 - Define information security roles and responsibilities	Manual, Disabled	1.1.0 ↗
Identify individuals with security roles and responsibilities ↗	CMA_C1566 - Identify individuals with security roles and responsibilities	Manual, Disabled	1.1.1 ↗
Integrate risk management process into SDLC ↗	CMA_C1567 - Integrate risk management process into SDLC	Manual, Disabled	1.1.0 ↗

## Acquisition Process

ID: NIST SP 800-53 Rev. 4 SA-4 Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Determine supplier contract obligations ↗	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	1.1.0 ↗
Document acquisition contract acceptance criteria ↗	CMA_0187 - Document acquisition contract acceptance criteria	Manual, Disabled	1.1.0 ↗
Document protection of personal data in acquisition contracts ↗	CMA_0194 - Document protection of personal data in acquisition contracts	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document protection of security information in acquisition contracts ↗	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document requirements for the use of shared data in contracts ↗	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	1.1.0 ↗
Document security assurance requirements in acquisition contracts ↗	CMA_0199 - Document security assurance requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document security documentation requirements in acquisition contract ↗	CMA_0200 - Document security documentation requirements in acquisition contract	Manual, Disabled	1.1.0 ↗
Document security functional requirements in acquisition contracts ↗	CMA_0201 - Document security functional requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document security strength requirements in acquisition contracts ↗	CMA_0203 - Document security strength requirements in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↗
Document the protection of cardholder data in third party contracts ↗	CMA_0207 - Document the protection of cardholder data in third party contracts	Manual, Disabled	1.1.0 ↗

## Functional Properties Of Security Controls

ID: NIST SP 800-53 Rev. 4 SA-4 (1) Ownership: Shared

[] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Obtain functional properties of security controls ↗	CMA_C1575 - Obtain functional properties of security controls	Manual, Disabled	1.1.0 ↗

# Design / Implementation Information For Security Controls

ID: NIST SP 800-53 Rev. 4 SA-4 (2) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Obtain design and implementation information for the security controls ↴	CMA_C1576 - Obtain design and implementation information for the security controls	Manual, Disabled	1.1.1 ↴

# Continuous Monitoring Plan

ID: NIST SP 800-53 Rev. 4 SA-4 (8) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Obtain continuous monitoring plan for security controls ↴	CMA_C1577 - Obtain continuous monitoring plan for security controls	Manual, Disabled	1.1.0 ↴

# Functions / Ports / Protocols / Services In Use

ID: NIST SP 800-53 Rev. 4 SA-4 (9) Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require developer to identify SDLC ports, protocols, and services ↴	CMA_C1578 - Require developer to identify SDLC ports, protocols, and services	Manual, Disabled	1.1.0 ↴

# Use Of Approved Piv Products

ID: NIST SP 800-53 Rev. 4 SA-4 (10) Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ FIPS 201-approved technology for PIV ↗</a>	CMA_C1579 - Employ FIPS 201-approved technology for PIV	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Information System Documentation

ID: NIST SP 800-53 Rev. 4 SA-5 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Distribute information system documentation ↗</a>	CMA_C1584 - Distribute information system documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Document customer-defined actions ↗</a>	CMA_C1582 - Document customer-defined actions	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Obtain Admin documentation ↗</a>	CMA_C1580 - Obtain Admin documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Obtain user security function documentation ↗</a>	CMA_C1581 - Obtain user security function documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Protect administrator and user documentation ↗</a>	CMA_C1583 - Protect administrator and user documentation	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## External Information System Services

ID: NIST SP 800-53 Rev. 4 SA-9 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Define and document government oversight ↗</a>	CMA_C1587 - Define and document government oversight	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require external service providers to comply with security requirements ↗</a>	CMA_C1586 - Require external service providers to comply with security requirements	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review cloud service provider's compliance with policies and agreements ↗	CMA_0469 - Review cloud service provider's compliance with policies and agreements	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Risk Assessments / Organizational Approvals

ID: NIST SP 800-53 Rev. 4 SA-9 (1) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assess risk in third party relationships ↗	CMA_0014 - Assess risk in third party relationships	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Obtain approvals for acquisitions and outsourcing ↗	CMA_C1590 - Obtain approvals for acquisitions and outsourcing	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Identification Of Functions / Ports / Protocols / Services

ID: NIST SP 800-53 Rev. 4 SA-9 (2) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Identify external service providers ↗	CMA_C1591 - Identify external service providers	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Consistent Interests Of Consumers And Providers

ID: NIST SP 800-53 Rev. 4 SA-9 (4) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Ensure external providers consistently meet interests of the customers ↴	CMA_C1592 - Ensure external providers consistently meet interests of the customers	Manual, Disabled	1.1.0 ↴

## Processing, Storage, And Service Location

ID: NIST SP 800-53 Rev. 4 SA-9 (5) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Restrict location of information processing, storage and services ↴	CMA_C1593 - Restrict location of information processing, storage and services	Manual, Disabled	1.1.0 ↴

## Developer Configuration Management

ID: NIST SP 800-53 Rev. 4 SA-10 Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Address coding vulnerabilities ↴	CMA_0003 - Address coding vulnerabilities	Manual, Disabled	1.1.0 ↴
Develop and document application security requirements ↴	CMA_0148 - Develop and document application security requirements	Manual, Disabled	1.1.0 ↴
Document the information system environment in acquisition contracts ↴	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↴
Establish a secure software development program ↴	CMA_0259 - Establish a secure software development program	Manual, Disabled	1.1.0 ↴
Perform vulnerability scans ↴	CMA_0393 - Perform vulnerability scans	Manual, Disabled	1.1.0 ↴
Remediate information system	CMA_0427 - Remediate information	Manual,	1.1.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">flaws ↗</a>	system flaws	Disabled	
<a href="#">Require developers to document approved changes and potential impact ↗</a>	CMA_C1597 - Require developers to document approved changes and potential impact	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require developers to implement only approved changes ↗</a>	CMA_C1596 - Require developers to implement only approved changes	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require developers to manage change integrity ↗</a>	CMA_C1595 - Require developers to manage change integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Software / Firmware Integrity Verification

ID: NIST SP 800-53 Rev. 4 SA-10 (1) Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Verify software, firmware and information integrity ↗</a>	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Developer Security Testing And Evaluation

ID: NIST SP 800-53 Rev. 4 SA-11 Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Perform vulnerability scans ↗</a>	CMA_0393 - Perform vulnerability scans	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Remediate information system flaws ↗</a>	CMA_0427 - Remediate information system flaws	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Require developers to produce evidence of security assessment plan execution ↗</a>	CMA_C1602 - Require developers to produce evidence of security assessment plan execution	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Supply Chain Protection

ID: NIST SP 800-53 Rev. 4 SA-12 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Assess risk in third party relationships ↗</a>	CMA_0014 - Assess risk in third party relationships	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Define requirements for supplying goods and services ↗</a>	CMA_0126 - Define requirements for supplying goods and services	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Determine supplier contract obligations ↗</a>	CMA_0140 - Determine supplier contract obligations	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Establish policies for supply chain risk management ↗</a>	CMA_0275 - Establish policies for supply chain risk management	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Development Process, Standards, And Tools

ID: NIST SP 800-53 Rev. 4 SA-15 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Review development process, standards and tools ↗</a>	CMA_C1610 - Review development process, standards and tools	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Developer-Provided Training

ID: NIST SP 800-53 Rev. 4 SA-16 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Require developers to provide training ↗</a>	CMA_C1611 - Require developers to provide training	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Developer Security Architecture And Design

ID: NIST SP 800-53 Rev. 4 SA-17 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require developers to build security architecture ↗	CMA_C1612 - Require developers to build security architecture	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to describe accurate security functionality ↗	CMA_C1613 - Require developers to describe accurate security functionality	Manual, Disabled	<a href="#">1.1.0 ↗</a>
Require developers to provide unified security protection approach ↗	CMA_C1614 - Require developers to provide unified security protection approach	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# System And Communications Protection

## System And Communications Protection Policy And Procedures

ID: NIST SP 800-53 Rev. 4 SC-1 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update system and communications protection policies and procedures ↗	CMA_C1616 - Review and update system and communications protection policies and procedures	Manual, Disabled	<a href="#">1.1.0 ↗</a>

# Application Partitioning

ID: NIST SP 800-53 Rev. 4 SC-2 Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Authorize remote access ↗</a>	CMA_0024 - Authorize remote access	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Separate user and information system management functionality ↗</a>	CMA_0493 - Separate user and information system management functionality	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Use dedicated machines for administrative tasks ↗</a>	CMA_0527 - Use dedicated machines for administrative tasks	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Security Function Isolation

ID: NIST SP 800-53 Rev. 4 SC-3 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Azure Defender for servers should be enabled ↗</a>	Azure Defender for servers provides real-time threat protection for server workloads and generates hardening recommendations as well as alerts about suspicious activities.	AuditIfNotExists, Disabled	<a href="#">1.0.3 ↗</a>
<a href="#">Endpoint protection solution should be installed on virtual machine scale sets ↗</a>	Audit the existence and health of an endpoint protection solution on your virtual machines scale sets, to protect them from threats and vulnerabilities.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Monitor missing Endpoint Protection in Azure Security Center ↗</a>	Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Windows Defender Exploit Guard should be enabled on your machines ↗</a>	Windows Defender Exploit Guard uses the Azure Policy Guest Configuration agent. Exploit Guard has four components that are designed to lock down devices against a wide variety of attack vectors and block behaviors commonly used in malware attacks while enabling enterprises to balance their security risk and productivity requirements (Windows only).	AuditIfNotExists, Disabled	<a href="#">2.0.0 ↗</a>

# Denial Of Service Protection

ID: NIST SP 800-53 Rev. 4 SC-5 Ownership: Shared

 Expand table

Name <small>(Azure portal)</small>	Description	Effect(s)	Version <small>(GitHub)</small>
<a href="#">Azure DDoS Protection Standard should be enabled ↗</a>	DDoS protection standard should be enabled for all virtual networks with a subnet that is part of an application gateway with a public IP.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Azure Web Application Firewall should be enabled for Azure Front Door entry-points ↗</a>	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.	Audit, Deny, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Develop and document a DDoS response plan ↗</a>	CMA_0147 - Develop and document a DDoS response plan	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">IP Forwarding on your virtual machine should be disabled ↗</a>	Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely required (e.g., when using the VM as a network virtual appliance), and therefore, this should be reviewed by the network security team.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">Web Application Firewall (WAF) should be enabled for Application Gateway ↗</a>	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP	Audit, Deny, Disabled	<a href="#">2.0.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
	address ranges, and other http(s) parameters via custom rules.		

## Resource Availability

ID: NIST SP 800-53 Rev. 4 SC-6 Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Govern the allocation of resources ↗	CMA_0293 - Govern the allocation of resources	Manual, Disabled	1.1.0 ↗
Manage availability and capacity ↗	CMA_0356 - Manage availability and capacity	Manual, Disabled	1.1.0 ↗
Secure commitment from leadership ↗	CMA_0489 - Secure commitment from leadership	Manual, Disabled	1.1.0 ↗

## Boundary Protection

ID: NIST SP 800-53 Rev. 4 SC-7 Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
[Preview]: All Internet traffic should be routed via your deployed Azure Firewall ↗	Azure Security Center has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall	AuditIfNotExists, Disabled	3.0.0-preview ↗
[Preview]: Storage account public access should be disallowed ↗	Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing	audit, Audit, deny, Deny, disabled, Disabled	3.1.0-preview ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	public access to a storage account unless your scenario requires it.		
<a href="#">Adaptive network hardening recommendations should be applied on internet facing virtual machines ↗</a>	Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">All network ports should be restricted on network security groups associated to your virtual machine ↗</a>	Azure Security Center has identified some of your network security groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↗</a>
<a href="#">API Management services should use a virtual network ↗</a>	Azure Virtual Network deployment provides enhanced security, isolation and allows you to place your API Management service in a non-internet routable network that you control access to. These networks can then be connected to your on-premises networks using various VPN technologies, which enables access to your backend services within the network and/or on-premises. The developer portal and API gateway, can be configured to be accessible either from the Internet or only within the virtual network.	Audit, Deny, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">App Configuration should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint ↗</a> .	AuditIfNotExists, Disabled	<a href="#">1.0.2 ↗</a>
<a href="#">Authorized IP ranges should be</a>	Restrict access to the Kubernetes Service Management API by granting API access	Audit, Disabled	<a href="#">2.0.1 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">defined on Kubernetes Services ↗</a>	only to IP addresses in specific ranges. It is recommended to limit access to authorized IP ranges to ensure that only applications from allowed networks can access the cluster.		
<a href="#">Azure API for FHIR should use private link ↗</a>	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> ↗ .	Audit, Disabled	1.0.0 ↗
<a href="#">Azure Cache for Redis should use private link ↗</a>	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
<a href="#">Azure Cognitive Search service should use a SKU that supports private link ↗</a>	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
<a href="#">Azure Cognitive Search services should disable public network access ↗</a>	Disabling public network access improves security by ensuring that your Azure Cognitive Search service is not exposed on the public internet. Creating private endpoints can limit exposure of your Search service. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
<a href="#">Azure Cognitive Search services</a>	Azure Private Link lets you connect your virtual network to Azure services without a	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should use private link ↗</a>	<p>public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.</p>		
<a href="#">Azure Cosmos DB accounts should have firewall rules ↗</a>	<p>Firewall rules should be defined on your Azure Cosmos DB accounts to prevent traffic from unauthorized sources. Accounts that have at least one IP rule defined with the virtual network filter enabled are deemed compliant. Accounts disabling public access are also deemed compliant.</p>	Audit, Deny, Disabled	<a href="#">2.0.0</a> ↗
<a href="#">Azure Data Factory should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a>.</p>	AuditIfNotExists, Disabled	<a href="#">1.0.0</a> ↗
<a href="#">Azure Event Grid domains should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> ↗.</p>	Audit, Disabled	<a href="#">1.0.2</a> ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Event Grid topics should use private link ↴	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> .	Audit, Disabled	1.0.2 ↴
Azure File Sync should use private link ↴	Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.	AuditIfNotExists, Disabled	1.0.0 ↴
Azure Key Vault should have firewall enabled ↴	Enable the key vault firewall so that the key vault is not accessible by default to any public IPs. Optionally, you can configure specific IP ranges to limit access to those networks. Learn more at: <a href="https://docs.microsoft.com/azure/key-vault/general/network-security">https://docs.microsoft.com/azure/key-vault/general/network-security</a>	Audit, Deny, Disabled	3.2.1 ↴
Azure Key Vaults should use private link ↴	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink</a> .	[parameters('audit_effect')]	1.2.1 ↴
Azure Machine Learning workspaces	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform	Audit, Disabled	1.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should use private link ↗</a>	handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .		
<a href="#">Azure Service Bus namespaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
<a href="#">Azure SignalR Service should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .	Audit, Disabled	1.0.0 ↗
<a href="#">Azure Synapse workspaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a> .	Audit, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Web Application Firewall should be enabled for Azure Front Door entry-points ↴	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.	Audit, Deny, Disabled	1.0.2 ↴
Azure Web PubSub Service should use private link ↴	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks.  Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a> ↴ .	Audit, Disabled	1.0.0 ↴
Cognitive Services accounts should disable public network access ↴	To improve the security of Cognitive Services accounts, ensure that it isn't exposed to the public internet and can only be accessed from a private endpoint. Disable the public network access property as described in <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> ↴ . This option disables access from any public address space outside the Azure IP range, and denies all logins that match IP or virtual network-based firewall rules. This reduces data leakage risks.	Audit, Deny, Disabled	3.0.1 ↴
Cognitive Services accounts should restrict network access ↴	Network access to Cognitive Services accounts should be restricted. Configure network rules so only applications from allowed networks can access the Cognitive Services account. To allow connections from specific internet or on-premises clients, access can be granted to traffic	Audit, Deny, Disabled	3.0.0 ↴

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
	from specific Azure virtual networks or to public internet IP address ranges.		
Cognitive Services should use private link <a href="#">↗</a>	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage. Learn more about private links at: <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> .	Audit, Disabled	3.0.0 <a href="#">↗</a>
Container registries should not allow unrestricted network access <a href="#">↗</a>	Azure container registries by default accept connections over the internet from hosts on any network. To protect your registries from potential threats, allow access from only specific private endpoints, public IP addresses or address ranges. If your registry doesn't have network rules configured, it will appear in the unhealthy resources. Learn more about Container Registry network rules here: <a href="https://aka.ms/acr/privatelink">https://aka.ms/acr/privatelink</a> , <a href="https://aka.ms/acr/portal/public-network">https://aka.ms/acr/portal/public-network</a> and <a href="https://aka.ms/acr/vnet">https://aka.ms/acr/vnet</a> .	Audit, Deny, Disabled	2.0.0 <a href="#">↗</a>
Container registries should use private link <a href="#">↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a> .	Audit, Disabled	1.0.1 <a href="#">↗</a>
CosmosDB accounts should use private link <a href="#">↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the	Audit, Disabled	1.0.0 <a href="#">↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at:  <a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a>.</p>		
Disk access resources should use private link ↗	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at:  <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a>.</p>	AuditIfNotExists, Disabled	1.0.0 ↗
Event Hub namespaces should use private link ↗	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at:  <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a>.</p>	AuditIfNotExists, Disabled	1.0.0 ↗
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	1.1.0 ↗
Internet-facing virtual machines should be protected with network security groups	<p>Protect your virtual machines from potential threats by restricting access to them with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsg-doc">https://aka.ms/nsg-doc</a></p>	AuditIfNotExists, Disabled	3.0.0 ↗
IoT Hub device provisioning service instances should use private link ↗	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the</p>	Audit, Disabled	1.0.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">Private endpoint connections on Azure IoT Hub should be enabled for your device</a>	<p>Private endpoint connections on Azure IoT Hub allow you to connect to your IoT Hub device from your private network. By using private endpoints, traffic is encrypted and sent directly to your IoT Hub device, bypassing the public internet. This provides a more secure way to send and receive data from your device.</p> <p>When using private endpoints, you can map private IP ranges to specific IoT Hub devices. This allows you to control who has access to your device and what traffic is sent to it. It also reduces the risk of data leakage by preventing unauthorized access to your device's data.</p> <p>To learn more about private links, see <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a>.</p>	AuditIfNotExists, Disabled	3.0.0 ↗
<a href="#">IP Forwarding on your virtual machine should be disabled</a>	<p>Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely required (e.g., when using the VM as a network virtual appliance), and therefore, this should be reviewed by the network security team.</p>	AuditIfNotExists, Disabled	3.0.0 ↗
<a href="#">Management ports of virtual machines should be protected with just-in-time network access control</a>	<p>Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations</p>	AuditIfNotExists, Disabled	3.0.0 ↗
<a href="#">Management ports should be closed on your virtual machines</a>	<p>Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine.</p>	AuditIfNotExists, Disabled	3.0.0 ↗
<a href="#">Non-internet-facing virtual machines should be protected with network security groups</a>	<p>Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsg-doc">https://aka.ms/nsg-doc</a></p>	AuditIfNotExists, Disabled	3.0.0 ↗
<a href="#">Private endpoint connections on Azure SQL Database should be enabled</a>	<p>Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.</p>	Audit, Disabled	1.1.0 ↗
<a href="#">Private endpoint should be enabled for MariaDB servers</a>	<p>Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and</p>	AuditIfNotExists, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	prevent access from all other IP addresses, including within Azure.		
Private endpoint should be enabled for MySQL servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for PostgreSQL servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Public network access on Azure SQL Database should be disabled ↴	Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP or virtual network based firewall rules.	Audit, Deny, Disabled	1.1.0 ↗
Public network access should be disabled for MariaDB servers ↴	Disable the public network access property to improve security and ensure your Azure Database for MariaDB can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↗
Public network access should be disabled for MySQL servers ↴	Disable the public network access property to improve security and ensure your Azure Database for MySQL can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↗
Public network access should be	Disable the public network access property to improve security and ensure your Azure	Audit, Deny, Disabled	2.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">disabled for PostgreSQL servers ↗</a>	Database for PostgreSQL can only be accessed from a private endpoint. This configuration disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.		
<a href="#">Storage accounts should restrict network access ↗</a>	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges	Audit, Deny, Disabled	1.1.1 ↗
<a href="#">Storage accounts should restrict network access using virtual network rules ↗</a>	Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.	Audit, Deny, Disabled	1.0.1 ↗
<a href="#">Storage accounts should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview</a> ↗	AuditIfNotExists, Disabled	2.0.0 ↗
<a href="#">Subnets should be associated with a Network Security Group ↗</a>	Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.	AuditIfNotExists, Disabled	3.0.0 ↗
<a href="#">VM Image Builder templates should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private	Audit, Disabled, Deny	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a> .			
<a href="#">Web Application Firewall (WAF) should be enabled for Application Gateway ↗</a>	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.	Audit, Deny, Disabled	2.0.0 ↗

## Access Points

ID: NIST SP 800-53 Rev. 4 SC-7 (3) Ownership: Shared

[ ] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">[Preview]: All Internet traffic should be routed via your deployed Azure Firewall ↗</a>			
<a href="#">[Preview]: All Internet traffic should be routed via your deployed Azure Firewall ↗</a>	Azure Security Center has identified that some of your subnets aren't protected with a next generation firewall. Protect your subnets from potential threats by restricting access to them with Azure Firewall or a supported next generation firewall	AuditIfNotExists, Disabled	3.0.0-preview ↗
<a href="#">[Preview]: Storage account public access should be disallowed ↗</a>	Anonymous public read access to containers and blobs in Azure Storage is a convenient way to share data but might present security risks. To prevent data breaches caused by undesired anonymous access, Microsoft recommends preventing	audit, Audit, deny, Deny, disabled, Disabled	3.1.0-preview ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	public access to a storage account unless your scenario requires it.		
Adaptive network hardening recommendations should be applied on internet facing virtual machines ↗	Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface	AuditIfNotExists, Disabled	3.0.0 ↗
All network ports should be restricted on network security groups associated to your virtual machine ↗	Azure Security Center has identified some of your network security groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to target your resources.	AuditIfNotExists, Disabled	3.0.0 ↗
API Management services should use a virtual network ↗	Azure Virtual Network deployment provides enhanced security, isolation and allows you to place your API Management service in a non-internet routable network that you control access to. These networks can then be connected to your on-premises networks using various VPN technologies, which enables access to your backend services within the network and/or on-premises. The developer portal and API gateway, can be configured to be accessible either from the Internet or only within the virtual network.	Audit, Deny, Disabled	1.0.2 ↗
App Configuration should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your app configuration instances instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/appconfig/private-endpoint">https://aka.ms/appconfig/private-endpoint</a> ↗.	AuditIfNotExists, Disabled	1.0.2 ↗
Authorized IP ranges should be	Restrict access to the Kubernetes Service Management API by granting API access	Audit, Disabled	2.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">defined on Kubernetes Services ↗</a>	only to IP addresses in specific ranges. It is recommended to limit access to authorized IP ranges to ensure that only applications from allowed networks can access the cluster.		
<a href="#">Azure API for FHIR should use private link ↗</a>	Azure API for FHIR should have at least one approved private endpoint connection. Clients in a virtual network can securely access resources that have private endpoint connections through private links. For more information, visit: <a href="https://aka.ms/fhir-privatelink">https://aka.ms/fhir-privatelink</a> ↗ .	Audit, Disabled	1.0.0 ↗
<a href="#">Azure Cache for Redis should use private link ↗</a>	Private endpoints lets you connect your virtual network to Azure services without a public IP address at the source or destination. By mapping private endpoints to your Azure Cache for Redis instances, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link">https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
<a href="#">Azure Cognitive Search service should use a SKU that supports private link ↗</a>	With supported SKUs of Azure Cognitive Search, Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Search service, data leakage risks are reduced. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
<a href="#">Azure Cognitive Search services should disable public network access ↗</a>	Disabling public network access improves security by ensuring that your Azure Cognitive Search service is not exposed on the public internet. Creating private endpoints can limit exposure of your Search service. Learn more at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗ .	Audit, Deny, Disabled	1.0.0 ↗
<a href="#">Azure Cognitive Search services</a>	Azure Private Link lets you connect your virtual network to Azure services without a	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should use private link ↗</a>	<p>public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Cognitive Search, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/azure-cognitive-search/inbound-private-endpoints">https://aka.ms/azure-cognitive-search/inbound-private-endpoints</a> ↗.</p>		
<a href="#">Azure Cosmos DB accounts should have firewall rules ↗</a>	<p>Firewall rules should be defined on your Azure Cosmos DB accounts to prevent traffic from unauthorized sources. Accounts that have at least one IP rule defined with the virtual network filter enabled are deemed compliant. Accounts disabling public access are also deemed compliant.</p>	Audit, Deny, Disabled	<a href="#">2.0.0</a> ↗
<a href="#">Azure Data Factory should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Data Factory, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/data-factory/data-factory-private-link">https://docs.microsoft.com/azure/data-factory/data-factory-private-link</a>.</p>	AuditIfNotExists, Disabled	<a href="#">1.0.0</a> ↗
<a href="#">Azure Event Grid domains should use private link ↗</a>	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid domain instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> ↗.</p>	Audit, Disabled	<a href="#">1.0.2</a> ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Event Grid topics should use private link ↗	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Event Grid topic instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/privateendpoints">https://aka.ms/privateendpoints</a> .	Audit, Disabled	1.0.2 ↗
Azure File Sync should use private link ↗	Creating a private endpoint for the indicated Storage Sync Service resource allows you to address your Storage Sync Service resource from within the private IP address space of your organization's network, rather than through the internet-accessible public endpoint. Creating a private endpoint by itself does not disable the public endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Key Vault should have firewall enabled ↗	Enable the key vault firewall so that the key vault is not accessible by default to any public IPs. Optionally, you can configure specific IP ranges to limit access to those networks. Learn more at: <a href="https://docs.microsoft.com/azure/key-vault/general/network-security">https://docs.microsoft.com/azure/key-vault/general/network-security</a>	Audit, Deny, Disabled	3.2.1 ↗
Azure Key Vaults should use private link ↗	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to key vault, you can reduce data leakage risks. Learn more about private links at: <a href="https://aka.ms/akvprivatelink">https://aka.ms/akvprivatelink</a> .	[parameters('audit_effect')]	1.2.1 ↗
Azure Machine Learning workspaces	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">should use private link ↗</a>	handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Machine Learning workspaces, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link">https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link</a> .		
<a href="#">Azure Service Bus namespaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Service Bus namespaces, data leakage risks are reduced. Learn more at: <a href="https://docs.microsoft.com/azure/service-bus-messaging/private-link-service">https://docs.microsoft.com/azure/service-bus-messaging/private-link-service</a> .	AuditIfNotExists, Disabled	1.0.0 ↗
<a href="#">Azure SignalR Service should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure SignalR Service resource instead of the entire service, you'll reduce your data leakage risks. Learn more about private links at: <a href="https://aka.ms/asrs/privatelink">https://aka.ms/asrs/privatelink</a> .	Audit, Disabled	1.0.0 ↗
<a href="#">Azure Synapse workspaces should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Azure Synapse workspace, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links">https://docs.microsoft.com/azure/synapse-analytics/security/how-to-connect-to-workspace-with-private-links</a> .	Audit, Disabled	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Web Application Firewall should be enabled for Azure Front Door entry-points ↴	Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.	Audit, Deny, Disabled	1.0.2 ↴
Azure Web PubSub Service should use private link ↴	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your Azure Web PubSub Service, you can reduce data leakage risks.  Learn more about private links at: <a href="https://aka.ms/awps/privatelink">https://aka.ms/awps/privatelink</a> .	Audit, Disabled	1.0.0 ↴
Cognitive Services accounts should disable public network access ↴	To improve the security of Cognitive Services accounts, ensure that it isn't exposed to the public internet and can only be accessed from a private endpoint. Disable the public network access property as described in <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> . This option disables access from any public address space outside the Azure IP range, and denies all logins that match IP or virtual network-based firewall rules. This reduces data leakage risks.	Audit, Deny, Disabled	3.0.1 ↴
Cognitive Services accounts should restrict network access ↴	Network access to Cognitive Services accounts should be restricted. Configure network rules so only applications from allowed networks can access the Cognitive Services account. To allow connections from specific internet or on-premises clients, access can be granted to traffic	Audit, Deny, Disabled	3.0.0 ↴

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
	from specific Azure virtual networks or to public internet IP address ranges.		
Cognitive Services should use private link <a href="#">🔗</a>	Azure Private Link lets you connect your virtual networks to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Cognitive Services, you'll reduce the potential for data leakage. Learn more about private links at: <a href="https://go.microsoft.com/fwlink/?linkid=2129800">https://go.microsoft.com/fwlink/?linkid=2129800</a> .	Audit, Disabled	3.0.0 <a href="#">🔗</a>
Container registries should not allow unrestricted network access <a href="#">🔗</a>	Azure container registries by default accept connections over the internet from hosts on any network. To protect your registries from potential threats, allow access from only specific private endpoints, public IP addresses or address ranges. If your registry doesn't have network rules configured, it will appear in the unhealthy resources. Learn more about Container Registry network rules here: <a href="https://aka.ms/acr/privatelink">https://aka.ms/acr/privatelink</a> , <a href="https://aka.ms/acr/portal/public-network">https://aka.ms/acr/portal/public-network</a> and <a href="https://aka.ms/acr/vnet">https://aka.ms/acr/vnet</a> .	Audit, Deny, Disabled	2.0.0 <a href="#">🔗</a>
Container registries should use private link <a href="#">🔗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The private link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your container registries instead of the entire service, you'll also be protected against data leakage risks. Learn more at: <a href="https://aka.ms/acr/private-link">https://aka.ms/acr/private-link</a> .	Audit, Disabled	1.0.1 <a href="#">🔗</a>
CosmosDB accounts should use private link <a href="#">🔗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the	Audit, Disabled	1.0.0 <a href="#">🔗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>consumer and services over the Azure backbone network. By mapping private endpoints to your CosmosDB account, data leakage risks are reduced. Learn more about private links at:  <a href="https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints">https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints</a>.</p>		
Disk access resources should use private link ↗	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to diskAccesses, data leakage risks are reduced. Learn more about private links at:  <a href="https://aka.ms/disksprivatelinksdoc">https://aka.ms/disksprivatelinksdoc</a>.</p>	AuditIfNotExists, Disabled	1.0.0 ↗
Event Hub namespaces should use private link ↗	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to Event Hub namespaces, data leakage risks are reduced. Learn more at:  <a href="https://docs.microsoft.com/azure/event-hubs/private-link-service">https://docs.microsoft.com/azure/event-hubs/private-link-service</a>.</p>	AuditIfNotExists, Disabled	1.0.0 ↗
Internet-facing virtual machines should be protected with network security groups ↗	<p>Protect your virtual machines from potential threats by restricting access to them with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsq-doc">https://aka.ms/nsq-doc</a></p>	AuditIfNotExists, Disabled	3.0.0 ↗
IoT Hub device provisioning service instances should use private link ↗	<p>Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to the IoT Hub device</p>	Audit, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	provisioning service, data leakage risks are reduced. Learn more about private links at: <a href="https://aka.ms/iotdpsvnet">https://aka.ms/iotdpsvnet</a> .		
<a href="#">IP Forwarding on your virtual machine should be disabled</a>	Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely required (e.g., when using the VM as a network virtual appliance), and therefore, this should be reviewed by the network security team.	AuditIfNotExists, Disabled	<a href="#">3.0.0</a>
<a href="#">Management ports of virtual machines should be protected with just-in-time network access control</a>	Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations	AuditIfNotExists, Disabled	<a href="#">3.0.0</a>
<a href="#">Management ports should be closed on your virtual machines</a>	Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine.	AuditIfNotExists, Disabled	<a href="#">3.0.0</a>
<a href="#">Non-internet-facing virtual machines should be protected with network security groups</a>	Protect your non-internet-facing virtual machines from potential threats by restricting access with network security groups (NSG). Learn more about controlling traffic with NSGs at <a href="https://aka.ms/nsq-doc">https://aka.ms/nsq-doc</a>	AuditIfNotExists, Disabled	<a href="#">3.0.0</a>
<a href="#">Private endpoint connections on Azure SQL Database should be enabled</a>	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	<a href="#">1.1.0</a>
<a href="#">Private endpoint should be enabled for MariaDB servers</a>	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MariaDB. Configure a private endpoint connection to enable access to traffic coming only from known networks and	AuditIfNotExists, Disabled	<a href="#">1.0.2</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	prevent access from all other IP addresses, including within Azure.		
Private endpoint should be enabled for MySQL servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for MySQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Private endpoint should be enabled for PostgreSQL servers ↴	Private endpoint connections enforce secure communication by enabling private connectivity to Azure Database for PostgreSQL. Configure a private endpoint connection to enable access to traffic coming only from known networks and prevent access from all other IP addresses, including within Azure.	AuditIfNotExists, Disabled	1.0.2 ↗
Public network access on Azure SQL Database should be disabled ↴	Disabling the public network access property improves security by ensuring your Azure SQL Database can only be accessed from a private endpoint. This configuration denies all logins that match IP or virtual network based firewall rules.	Audit, Deny, Disabled	1.1.0 ↗
Public network access should be disabled for MariaDB servers ↴	Disable the public network access property to improve security and ensure your Azure Database for MariaDB can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↗
Public network access should be disabled for MySQL servers ↴	Disable the public network access property to improve security and ensure your Azure Database for MySQL can only be accessed from a private endpoint. This configuration strictly disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.	Audit, Deny, Disabled	2.0.0 ↗
Public network access should be	Disable the public network access property to improve security and ensure your Azure	Audit, Deny, Disabled	2.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">disabled for PostgreSQL servers ↗</a>	Database for PostgreSQL can only be accessed from a private endpoint. This configuration disables access from any public address space outside of Azure IP range, and denies all logins that match IP or virtual network-based firewall rules.		
<a href="#">Storage accounts should restrict network access ↗</a>	Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges	Audit, Deny, Disabled	1.1.1 ↗
<a href="#">Storage accounts should restrict network access using virtual network rules ↗</a>	Protect your storage accounts from potential threats using virtual network rules as a preferred method instead of IP-based filtering. Disabling IP-based filtering prevents public IPs from accessing your storage accounts.	Audit, Deny, Disabled	1.0.1 ↗
<a href="#">Storage accounts should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private endpoints to your storage account, data leakage risks are reduced. Learn more about private links at - <a href="https://aka.ms/azureprivatelinkoverview">https://aka.ms/azureprivatelinkoverview</a> ↗	AuditIfNotExists, Disabled	2.0.0 ↗
<a href="#">Subnets should be associated with a Network Security Group ↗</a>	Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet.	AuditIfNotExists, Disabled	3.0.0 ↗
<a href="#">VM Image Builder templates should use private link ↗</a>	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or destination. The Private Link platform handles the connectivity between the consumer and services over the Azure backbone network. By mapping private	Audit, Disabled, Deny	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	<p>endpoints to your VM Image Builder building resources, data leakage risks are reduced. Learn more about private links at: <a href="https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet">https://docs.microsoft.com/azure/virtual-machines/linux/image-builder-networking#deploy-using-an-existing-vnet</a>.</p>		
<a href="#">Web Application Firewall (WAF) should be enabled for Application Gateway ↗</a>	<p>Deploy Azure Web Application Firewall (WAF) in front of public facing web applications for additional inspection of incoming traffic. Web Application Firewall (WAF) provides centralized protection of your web applications from common exploits and vulnerabilities such as SQL injections, Cross-Site Scripting, local and remote file executions. You can also restrict access to your web applications by countries, IP address ranges, and other http(s) parameters via custom rules.</p>	Audit, Deny, Disabled	2.0.0 ↗

## External Telecommunications Services

ID: NIST SP 800-53 Rev. 4 SC-7 (4) Ownership: Shared

[ ] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement managed interface for each external service ↗</a>	CMA_C1626 - Implement managed interface for each external service	Manual, Disabled	1.1.0 ↗
<a href="#">Implement system boundary protection ↗</a>	CMA_0328 - Implement system boundary protection	Manual, Disabled	1.1.0 ↗
<a href="#">Secure the interface to external systems ↗</a>	CMA_0491 - Secure the interface to external systems	Manual, Disabled	1.1.0 ↗

## Prevent Split Tunneling For Remote Devices

ID: NIST SP 800-53 Rev. 4 SC-7 (7) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Prevent split tunneling for remote devices ↗</a>	CMA_C1632 - Prevent split tunneling for remote devices	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Route Traffic To Authenticated Proxy Servers

ID: NIST SP 800-53 Rev. 4 SC-7 (8) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Route traffic through authenticated proxy network ↗</a>	CMA_C1633 - Route traffic through authenticated proxy network	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Host-Based Protection

ID: NIST SP 800-53 Rev. 4 SC-7 (12) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement system boundary protection ↗</a>	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Isolation Of Security Tools / Mechanisms / Support Components

ID: NIST SP 800-53 Rev. 4 SC-7 (13) Ownership: Shared

[\[+\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Isolate SecurID systems, Security Incident Management systems ↗</a>	CMA_C1636 - Isolate SecurID systems, Security Incident	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Management systems		

## Fail Secure

ID: NIST SP 800-53 Rev. 4 SC-7 (18) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Implement system boundary protection ↗</a>	CMA_0328 - Implement system boundary protection	Manual, Disabled	<a href="#">1.1.0 ↗</a>
<a href="#">Manage transfers between standby and active system components ↗</a>	CMA_0371 - Manage transfers between standby and active system components	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Dynamic Isolation / Segregation

ID: NIST SP 800-53 Rev. 4 SC-7 (20) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Ensure system capable of dynamic isolation of resources ↗</a>	CMA_C1638 - Ensure system capable of dynamic isolation of resources	Manual, Disabled	<a href="#">1.1.0 ↗</a>

## Isolation Of Information System Components

ID: NIST SP 800-53 Rev. 4 SC-7 (21) Ownership: Shared

[\[ \]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
<a href="#">Employ boundary protection to isolate information systems ↗</a>	CMA_C1639 - Employ boundary protection to isolate information	Manual, Disabled	<a href="#">1.1.0 ↗</a>

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
	systems		

## Transmission Confidentiality And Integrity

ID: NIST SP 800-53 Rev. 4 SC-8 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
<a href="#">App Service apps should only be accessible over HTTPS ↴</a>	Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.	Audit, Disabled, Deny	<a href="#">4.0.0 ↴</a>
<a href="#">App Service apps should require FTPS only ↴</a>	Enable FTPS enforcement for enhanced security.	AuditIfNotExists, Disabled	<a href="#">3.0.0 ↴</a>
<a href="#">App Service apps should use the latest TLS version ↴</a>	Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the latest TLS version for App Service apps to take advantage of security fixes, if any, and/or new functionalities of the latest version.	AuditIfNotExists, Disabled	<a href="#">2.0.1 ↴</a>
<a href="#">Azure HDInsight clusters should use encryption in transit to encrypt communication between Azure HDInsight cluster nodes ↴</a>	Data can be tampered with during transmission between Azure HDInsight cluster nodes. Enabling encryption in transit addresses problems of misuse and tampering during this transmission.	Audit, Deny, Disabled	<a href="#">1.0.0 ↴</a>
<a href="#">Enforce SSL connection should be enabled for MySQL database servers ↴</a>	Azure Database for MySQL supports connecting your Azure Database for MySQL server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between your database server and your client applications helps protect against 'man in the middle' attacks by encrypting the data stream between the server and your application. This	Audit, Disabled	<a href="#">1.0.1 ↴</a>