

individual access policies for each service's managed identity:

- APIM can get the host key of the Patient API function app.
- The Patient API function app can get the Audit API host key and the Azure Cosmos DB connection string for its data store.
- The Audit API function app can get the Azure Cosmos DB connection string for its data store.

Cost optimization

Cost optimization is about looking at ways to reduce unnecessary expenses and improve operational efficiencies. For more information, see [Overview of the cost optimization pillar](#).

One of the primary benefits of serverless applications like Azure Functions is the cost savings of paying only for consumption, rather than paying up front for dedicated servers. Virtual network support requires the [Azure Functions Premium](#) plan, at additional charge. Azure Functions Premium has support for regional virtual network integration, while still supporting dynamic scaling. The Azure Functions Premium SKU includes virtual network integration on APIM.

For details and pricing calculator, see [Azure Functions pricing](#).

Functions can also be hosted on [App Service virtual machines](#). Only [App Service Environments \(ASEs\)](#) offer complete network-level virtual network isolation. ASEs can be considerably more expensive than an Azure Functions plan that supports regional virtual network integration, and ASE scaling is less elastic.

Deploy this scenario

The source code for this solution is at [Azure VNet-Integrated Serverless Microservices](#).

The [TypeScript](#) source code for the [PatientTest API](#) and the [Audit API](#) are in the `/src` folder. Each API's source includes a [dev container](#) that has all the prerequisites installed, to help you get going quickly.

Both APIs have a full suite of automated integration and unit tests to help prevent regressions when you make changes. The project is also configured for *linting* with ESLint, to maintain code styles and help guard against unintentional errors. The services' respective README files contain information on how to run the tests and linting.

Terraform deployment

The code project's [/env](#) folder includes scripts and templates for [Terraform](#) deployment. Terraform deploys APIM and the function apps, and configures them to use the deployed Application Insights instance. Terraform also provisions all resources and configurations, including networking lockdown and the access key security pattern.

The deployment [README](#) explains how to deploy the Terraform environment in your own Azure subscription. The `/env` folder also includes a [dev container](#) that has all the prerequisites installed for Terraform deployment.

Locust load testing

To gauge API performance, you can run load testing against the APIs with the included [Locust load tests](#). [Locust](#) is an open-source load testing tool, and the tests are written in Python. You can run the load tests locally, or remotely in an Azure Kubernetes Service (AKS) cluster. The tests perform a variety of operations against the APIM endpoint, and verify behaviors against success and failure criteria.

Contributors

This article is maintained by Microsoft. It was originally written by the following contributors.

Principal author:

- [Hannes Nel](#) | Principal Software Engineering Lead

To see non-public LinkedIn profiles, sign in to LinkedIn.

Next steps

- [Use Azure API Management with microservices deployed in Azure Kubernetes Service](#)
- [How to use Azure API Management with virtual networks](#)
- [How to use managed identities for App Service and Azure Functions](#)
- [Use Key Vault references for App Service and Azure Functions](#)
- [APIs and microservices e-book](#)
- [API Management access restriction policies](#)
- [Azure Functions networking options](#)
- [Azure Functions scale and hosting](#)

Related resources

The following architectures cover key API Management scenarios:

- [Migrate a web app using Azure API Management](#)
- [Protect APIs with Application Gateway and API Management](#)
- [Azure API Management landing zone accelerator](#)

The following articles cover key functions scenarios:

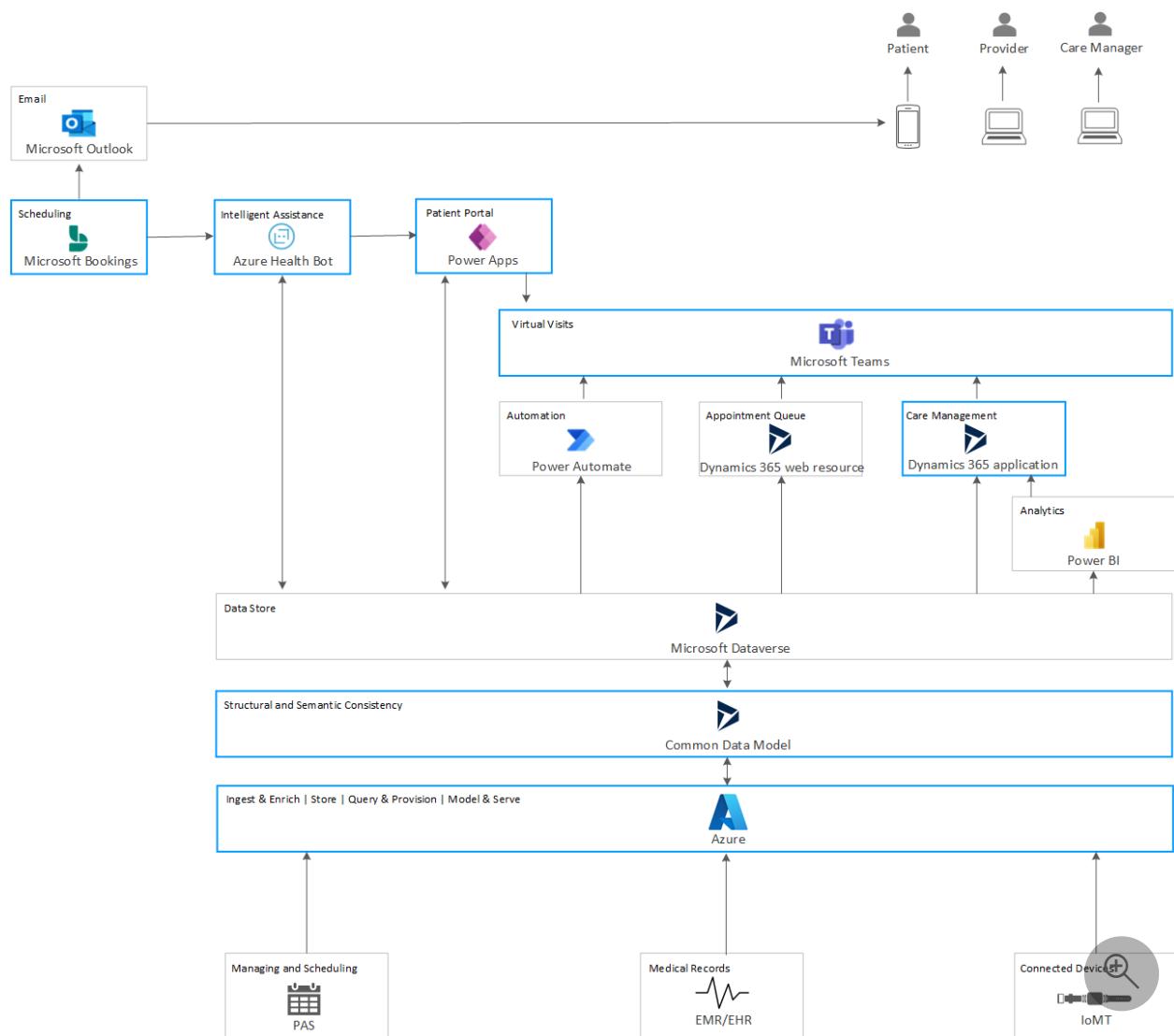
- [Integrate Event Hubs with serverless functions on Azure](#)
- [Monitor Azure Functions and Event Hubs](#)
- [Azure Functions in a hybrid environment](#)
- [Performance and scale for Event Hubs and Azure Functions](#)
- [Code walkthrough: Serverless application with Functions](#)
- [Azure App Service and Azure Functions considerations for multitenancy](#)

Virtual health on Microsoft Cloud for Healthcare

Azure

This article discusses a potential solution for scheduling and following up on virtual visits between patients, providers, and care managers.

Architecture



Download a [Visio file](#) that contains this architecture diagram.

In this architecture diagram, the blue-lined boxes represent the Microsoft services that are either the underlying services or add-ons required for [Microsoft Cloud for Healthcare](#), each of which must be licensed separately. These components together

help speed up development of integrated healthcare solutions for patient engagement, health team collaboration, and improvement of clinical and operational data insights.

The data flows into the system through various external medical systems, such as patient and provider schedules, medical records, wearable devices, and so on. This data is ingested using Azure. It is then stored in the Microsoft Dataverse, a data store powered by the Power Apps Platform. This data is formatted to use entities and relationships between them, created using the [Common Data Model \(CDM\)](#), an industry standard to represent medical data. All interactions between patient, provider, and the care manager happen using this CDM data stored in Dataverse.

An established patient can log in securely to the Patient Portal, a website hosted in the Power Apps Portals. In this portal, the patient can talk to an *Intelligent Assistant*. This is an instance of the [Azure Health Bot service](#), which gathers their symptoms, provides suggestions, and recommends calling to the practitioner, if needed. If the patient chooses to connect to their medical provider, the health bot instance gets the data on providers available for virtual visits and their schedules, from the Dataverse. Once the patient selects a provider and a time, the bot presents their contact information, obtained from the *EMR/EHR* data stored in Dataverse. The patient can validate or change this information, and save the data using the bot.

To schedule an appointment, the health bot instance connects to the Bookings App using the [Microsoft Graph API](#) and books an appointment on the provider's calendar. An email with the appointment information is sent to both the parties using Microsoft Outlook. The patient is given instructions to log in to the Patient Portal for the intake process. This process involves confirming or changing their contact, payment, and insurance information, and then signing a consent form for the virtual visit. Once they sign the consent, they are provided the Microsoft Teams link for the appointment.

The provider logs into Teams to check their appointment schedule and summary information for each. Teams presents this information using the *Appointment Queue* application. The provider is then able to start the virtual visit on Teams for the scheduled appointment. During the call, the provider can take notes and add them to the patient's records.

A new note on the patient's medical records triggers a review notification for the care manager assigned to the patient. When the care manager receives this notification, they can log in to Teams, where they are able to see the patients assigned to them, and view the notes. Through the Care Management app, they can make required changes to the patient's care plan.

Components

The architecture consists of the following components:

- **PAS.** Patient Administration Systems (PAS) are systems that automate the administrative paperwork in healthcare organizations, such as hospitals. They are the core components of the IT infrastructure of such an organization. A PAS records the patient's demographics, such as name, home address, date of birth, and so on. It also records detailed information of all contact the patient had with the hospital, both outpatient and inpatient. With the help of PAS, modern hospitals are able to report and schedule resources across the organization. PAS is a key source of scheduling data in this solution. Since this data is external and may be in a non-standard format, it is important to convert it into a format that is understood by all components of this solution.
- **EMR/EHR.** [Electronic Medical Records \(EMR\)](#) and [Electronic Health Records \(EHR\)](#) provide the digital records of a patient's medical and health information, including diagnoses, medications, immunizations, and so on. They can be scoped to a single practice office, such as EMRs, or designed to scope much larger, traveling with the patients to whichever facility they go, such as the EHRs. These are important external data sources in this solution, and may be unstructured non-standard format. As such, this data needs to be converted to a format that can be used by the components in this solution.
- **Azure API for FHIR.** Azure is the first step in the process of bringing data into the Microsoft ecosystem and the Microsoft Cloud for Healthcare. This layer provides a secure interface between external data and internal components of this architecture. The Azure API for FHIR ingests the data coming from disparate sources such as EMR, PAS, devices, whether structured or unstructured, converts it into FHIR and persists in Azure. This data can then be used across the Microsoft Cloud for Healthcare for different services. The Azure API for FHIR is built with security and compliance in mind and designed for PHI (Protected Health Information) data. For more information on this layer, see [Azure for healthcare](#) and the [Azure API for FHIR](#)
- **Common Data Model.** With [Common Data Model](#), Microsoft provides a standardized metadata definition system that is extensible and customizable for specific business needs. CDM entities are available for subject areas such as, CRM, Healthcare, Talent, and so on. For details, read the [Common Data Model usage information](#). In addition to these entities, customers can pull in proprietary data by defining that entity table and the underlying fields in the Common Data Model, which can then seamlessly be used with other entities throughout their solution.

- **Microsoft Dataverse.** [Dataverse](#), a relational database that powers Microsoft Dynamics 365, is the repository for the data represented in the Common Data Model. It holds databases for patient information, containing details about their names, family information, medical conditions, medication history, and so on. It also holds the information obtained from any wearable devices used and registered by the patients, as well as, scheduling and management data from the healthcare organization. This data is defined using the Common Data Model.
- **Patient Portal.** This [Power Apps portal](#) lets patients view their medical records, book appointments, chat with the health bot instance, and so on. This portal can be extended to support other data. This portal is part of Microsoft Cloud for Healthcare, and allows you to easily spin up a portal, which can connect with entities in Dataverse, pulling in data such as patient information, care plans, appointments, and so on.
- **Intelligent Assistance.** This is an instance of the [Azure Health Bot Service](#), accessible to patients through the Patient Portal. This health bot instance is loaded within an Azure App Service website. It is customizable, and can be programmed using the scenarios required by the customers.
- **Bookings App.** Bookings App is a Microsoft 365 service, included in the Microsoft Cloud for Healthcare. It facilitates scheduling of calendar events, and allows creating Teams meetings.
- **Microsoft Outlook.** This solution uses [Microsoft Outlook](#) as the email client. The Bookings App that sends the email notification is integrated with Outlook. Alternatively, the healthcare provider's preferred email client may be used.
- **Microsoft Teams.** [Microsoft Teams](#) is a component of Microsoft Cloud for Healthcare, and provides the front end for interactions between the patients, providers, and care managers. Users can use a locally installed version or the web version. For more information on Teams, read the [Microsoft Teams documentation](#).
- **Appointment Queue.** This tool generates an HTML page with data pulled out of the Dataverse, using the [Dynamics 365 Web API](#). It presents the provider with information about the appointments scheduled for the day and summary about each. It also provides a link to access the patient information through the Care Management application. The Appointment Queue was developed to support this scenario, and is not a part of Microsoft Cloud for Healthcare. The data sources for this tool are mainly the PAS systems and EMR/EHR records. If these systems have tools integrated to present this data, those tools may be a replacement for this component in an actual deployment.

- **Care Management.** The Care Management tool is a component of Microsoft Cloud for Healthcare. It is a Power Apps application deployed through Dynamics 365. It pulls in the EMR/EHR patient data stored in the Dataverse in CDM format, and presents an aggregated view in Teams. A care center's solution might choose to use their own system for their functionality, depending on how they want to present this information.
- **Power BI Analytics**  . This is an analytics tool created for this scenario, and is not available with Microsoft Cloud for Healthcare. In this solution, it generates information derived from the patient's IoMT devices. This could be data such as heart rate, blood oxygen level, and so on. The Care Management app uses this data to present medical providers with additional insights about their patients based on their daily activities.
- **Connected devices.** These are *Internet of Medical Things (IoMT)* devices, which are smart devices for medical or healthcare use. Examples of IoMT devices include wearables such as Apple Watch or Fitbit, medical or vital monitors, and so on. Patients can provision their devices through Azure, and choose to allow their health care management system to gather this IoMT data for use by their providers. Providers can gain additional insights from such devices, in near real time, and link anomalies such as an elevated heart rate for a period of time, with patient's current symptoms.
- **Automation with Power Automate.** This is a custom tool created to support this scenario, and is not available with Microsoft Cloud for Healthcare. Since this is a virtual visit scenario, the provider might just be an on-call physician and not the patient's regular physician. This tool allows the provider's notes to trigger a Teams notification to the *care manager*. A care manager is the member of the medical team that works as the liaison between the primary care physician (PCP) and the patient, and takes care of long-term care management. A notification sent to the care manager, indicating new notes added for the patient, enables them to review and make appropriate changes in the patient's care management after the visit.

Alternatives

Azure for healthcare services such as Azure API for FHIR and Azure Health Bot, Common Data Model interface, Microsoft Dataverse, and Microsoft Teams form the core components of this solution. Most other components of this system can be replaced by systems currently used by the healthcare facility:

- If the EMR/EHR system comes with built-ins for booking, scheduling, and care management, these built-ins can be used instead of the corresponding

components in this solution.

- Bookings and Outlook scheduling and email notification could be swapped out by the systems used by the healthcare facility. These could be done via the EHR system, or using a third-party application. The application should provide an API that the health bot instance can use to create and schedule appointments, along with the capability to create virtual meetings.
- If the provider already has a patient portal implemented through their EMR/EHR system, it may be used instead of the Patient Portal. It is easy to integrate such an external component with this solution, since these components used standard interfaces, for example, an [iFrame](#) interface to communicate with the health bot instance. Components that support this flow can be created on the proprietary portal, such as the consent form that the patient needs to sign before joining the Teams meeting.
- It's worth noting that an actual deployment will need replacement tools for some components in this solution, such as the Appointment Queue, automated notifications, and Power BI analytics tools. These components will need to be created and customized for the healthcare provider's business needs.

Scenario details

In the current COVID-19 (coronavirus) pandemic, a large number of patients might prefer to visit their medical providers virtually rather than in person, whenever possible. Improving clinical and operational insights in healthcare becomes important in such a virtual world. This includes connecting data from across systems, creating insights to predict risk and help improve patient care, quality assurance, and operational efficiencies.

The foundation for this solution is the [Microsoft Cloud for Healthcare](#). Microsoft Cloud for Healthcare brings together trusted capabilities from Microsoft 365, Azure, Dynamics 365, Power Platform, and Microsoft's extensive partner ecosystem to help healthcare organizations create fast, efficient, and secure healthcare solutions.

Potential use cases

This solution is targeted to provide virtual patient care in the current pandemic. However, health care providers can easily apply it to the following scenarios:

- Scheduling virtual follow-ups to in person visits.

- Providing non-emergency medical guidance to patients while traveling.

Considerations

These considerations implement the pillars of the Azure Well-Architected Framework, which is a set of guiding tenets that can be used to improve the quality of a workload. For more information, see [Microsoft Azure Well-Architected Framework](#).

Security

Security provides assurances against deliberate attacks and the abuse of your valuable data and systems. For more information, see [Overview of the security pillar](#).

Since the system is built around patient data, basic security considerations for private information should be applied when developing this solution:

- Only the required data should flow through the system at any given time. For example, pull in only that data from the EMR/EHR systems that is required to surface for the virtual visit scheduling and management. Review the established [HIPAA compliance rules](#) for guidance on where the patient data should be stored, what can be done with it, and who should have access to it. Be aware of the importance of compliance in healthcare while developing your solution. For further guidance, read [Compliance in Microsoft Cloud for Healthcare](#).
- Only authorized personnel should have access to patient data, and only to the data required for their role. At various points in the system, such as the Care Management and the analytics feeding into it, the Appointment Queue, or the notification systems, care should be taken to authenticate and authorize personnel, and limit their access to only the required patient information.
- Modules interacting with patients, such as the Intelligent Assistance and Bookings app, take in, store, and use patient data. Proper access control and authentication at these modules ensures privacy concerns are addressed.

Because of the nature of private data involved, [security](#) and [compliance](#) form the basic tenets of Microsoft Cloud for Healthcare.

This example also relies on the security rules set by Dynamics 365 and Teams:

- [Dynamics 365 security](#)
- [Microsoft Teams security](#)

Individual services included in Microsoft Cloud for Healthcare provide their own layer of security and compliance:

- [Power Platform compliance and data privacy](#)
- [Dataverse security](#)

For custom security controls, consider using [Microsoft Entra ID](#) and [role-based access control](#).

Finally, when implementing this solution, keep in mind the [best practices and guidance for developing secure Azure solutions](#).

Cost optimization

Cost optimization is about looking at ways to reduce unnecessary expenses and improve operational efficiencies. For more information, see [Overview of the cost optimization pillar](#).

For detailed pricing information on Microsoft Cloud for Healthcare, see [How to buy Microsoft Cloud for Healthcare](#). The components that form the Microsoft Cloud for Healthcare, have their own licensing requirement, such as:

- [Microsoft 365 pricing plans](#)
- [Microsoft Dynamics 365 pricing](#)

To recreate components in this architecture that were custom-made, consider the pricing information for the underlying services that you choose to use.

Deploy this scenario

The solution should be deployed in stages:

1. Some products/services must be installed as the prerequisites for Microsoft Cloud for Healthcare. See the detailed list on [this article on licensing requirements](#).
2. Microsoft Cloud for Healthcare can be deployed using instructions provided in the [Deploy Microsoft Cloud for Healthcare solutions powered by Dynamics 365](#).
3. Microsoft Cloud for Healthcare provides basic components to jumpstart building a virtual health solution, such as, Patient Portal, Teams, Bookings, and so on. The data that will be used to power these building blocks, should be customized as per the business needs.

4. The components available in Microsoft Cloud for Healthcare and its prerequisites, should be customized to support the business needs:
 - a. Power Automate flows should be created to support the care manager notifications.
 - b. Patient Portal should be configured. Additional forms might need to be created for elements such as the check-in/consent forms. Read [Set up and configure a Patient Access portal](#) for more information.
 - c. Azure Health Bot service should be connected to the Dataverse database, and customized for its communication with patients. Read [Configure automatic chats using Microsoft Health Bot](#) for more information.
 - d. See [Configure sync with clinical data using Azure FHIR Sync Agent](#) and [Embed Power BI reports for analytics](#) to understand some other configurations that may be required.
5. The additional components that were specifically created for this solution, are not available for production-grade usage. The healthcare facility may need to create its own version of these applications:
 - a. Appointment Queue
 - b. Automated notifications using Power Automate
 - c. Reporting application using Power BI

Contributors

This article is maintained by Microsoft. It was originally written by the following contributors.

Principal authors:

- [Slavica Frljanic](#) | Principal Group Program Manager
- [Dhanashri Kshirsagar](#) | Senior Content PM

To see non-public LinkedIn profiles, sign in to LinkedIn.

Next steps

- [What is Microsoft Cloud for Healthcare?](#)

- Learn more about Azure for healthcare offerings at [Azure for Healthcare—Healthcare Solutions](#)
- Difference between EMR and EHR
- HIPAA compliance rules
- What is Azure API for FHIR?
- What is Microsoft Dataverse?
- What is the Azure Health Bot Service?
- What is Power BI?
- Learn how you can use [Microsoft Dynamics 365](#)

Related resources

- Clinical and medical insights using Microsoft Cloud for Healthcare
- Consumer health portal on Azure
- HIPAA and HITRUST compliant health data AI

Bing COVID-19

Article • 05/05/2023

Bing COVID-19 data includes confirmed, fatal, and recovered cases from all regions, updated daily. This data is reflected in the [Bing COVID-19 Tracker](#).

Bing collects data from multiple trusted, reliable sources, including the [World Health Organization \(WHO\)](#), [Centers for Disease Control and Prevention \(CDC\)](#), national/regional and state public health departments, [BNO News](#), [24/7 Wall St.](#), and [Wikipedia](#).

ⓘ Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Datasets

Modified datasets are available in CSV, JSON, JSON-Lines, and Parquet.

- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/bing_covid-19_data/latest/bing_covid-19_data.csv
- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/bing_covid-19_data/latest/bing_covid-19_data.json
- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/bing_covid-19_data/latest/bing_covid-19_data.jsonl
- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/bing_covid-19_data/latest/bing_covid-19_data.parquet

All modified datasets have ISO 3166 subdivision codes and load times added, and use lower case column names with underscore separators.

Raw data: https://pandemicdatalake.blob.core.windows.net/public/raw/covid-19/bing_covid-19_data/latest/Bing-COVID19-Data.csv

Previous versions of modified and raw data: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/bing_covid-19_data/

Data volume

All datasets are updated daily. As of May 11, 2020 they contained 125,576 rows (CSV 16.1 MB, JSON 40.0 MB, JSONL 39.6 MB, Parquet 1.1 MB).

License and use rights attribution

This data is available strictly for educational and academic purposes, such as medical research, government agencies, and academic institutions, under [terms and conditions](#).

Data used or cited in publications should include an attribution to 'Bing COVID-19 Tracker' with a link to www.bing.com/covid.

Contact

For any questions or feedback about this or other datasets in the COVID-19 Data Lake, please contact askcovid19dl@microsoft.com.

Columns

Name	Data type	Unique	Values (sample)	Description
admin_region_1	string	864	Texas Georgia	Region within country_region
admin_region_2	string	3,143	Washington County Jefferson County	Region within admin_region_1
confirmed	int	120,692	1 2	Confirmed case count for the region
confirmed_change	int	12,120	1 2	Change of confirmed case count from the previous day

Name	Data type	Unique	Values (sample)			Description				
country_region	string	237	United States India			Country/region				
deaths	int	20,616	1 2			Death case count for the region				
deaths_change	smallint	1,981	1 2			Change of death count from the previous day				
id	int	1,783,534	742546 69019298			Unique identifier				
iso_subdivision	string	484	US-TX US-GA			Two-part ISO subdivision code				
iso2	string	226	US IN			2 letter country code identifier				
iso3	string	226	USA IND			3 letter country code identifier				
latitude	double	5,675	42.28708 19.59852			Latitude of the centroid of the region				
load_time	timestamp	1	2021-04-26 00:06:34.719000			The date and time the file was loaded from the Bing source on GitHub				
longitude	double	5,693	-2.5396 -155.5186			Longitude of the centroid of the region				
recovered	int	73,287	1 2			Recovered count for the region				
recovered_change	int	10,441	1 2			Change of recovered case count from the previous day				
updated	date	457	2021-04-23 2021-04-22			The as at date for the record				

Preview

id	updated	confirmed	deaths	iso2	iso3	country_region	admin_region_1	iso_subdivision	admin_region_2	load_time	confirmed_change
338995	2020-01-21	262	0	null	null	Worldwide	null	null	null	4/26/2021 12:06:34 AM	
338996	2020-01-22	313	0	null	null	Worldwide	null	null	null	4/26/2021 12:06:34 AM	51
338997	2020-01-23	578	0	null	null	Worldwide	null	null	null	4/26/2021 12:06:34 AM	265
338998	2020-01-24	841	0	null	null	Worldwide	null	null	null	4/26/2021 12:06:34 AM	263
338999	2020-01-25	1320	0	null	null	Worldwide	null	null	null	4/26/2021 12:06:34 AM	479
339000	2020-01-26	2014	0	null	null	Worldwide	null	null	null	4/26/2021 12:06:34 AM	694
339001	2020-01-27	2798	0	null	null	Worldwide	null	null	null	4/26/2021 12:06:34 AM	784
339002	2020-01-28	4593	0	null	null	Worldwide	null	null	null	4/26/2021 12:06:34 AM	1795
339003	2020-01-29	6065	0	null	null	Worldwide	null	null	null	4/26/2021 12:06:34 AM	1472
339004	2020-01-30	7818	0	null	null	Worldwide	null	null	null	4/26/2021 12:06:34 AM	1753

Data access

Azure Notebooks

azure-storage

Tip

Download the notebook instead. .

This notebook documents the URLs and sample code to access the [Bing COVID-19 Dataset](#).

Use the following URLs to get specific file formats hosted on Azure Blob Storage:

CSV: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/bing_covid-19_data/latest/bing_covid-19_data.csv

JSON: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/bing_covid-19_data/latest/bing_covid-19_data.json

JSONL: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/bing_covid-19_data/latest/bing_covid-19_data.jsonl

Parquet: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/bing_covid-19_data/latest/bing_covid-19_data.parquet

Download the dataset file using the built-in capability download from an http URL in Pandas. Pandas has readers for various file formats:

https://pandas.pydata.org/pandas-docs/stable/reference/api/pandas.read_parquet.html

https://pandas.pydata.org/pandas-docs/stable/reference/api/pandas.read_csv.html

Python

```
import pandas as pd
import numpy as np
%matplotlib inline
import matplotlib.pyplot as plt

df = pd.read_parquet("https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/bing_covid-19_data/latest/bing_covid-19_data.parquet")
df.head(10)
```

Lets check the data types of the various fields and verify that the updated column is datetime format

Python

```
df.dtypes
```

We will now look into Worldwide data and plot some simple charts to visualize the data

Python

```
df_Worldwide=df[df['country_region']=='Worldwide']
```

Python

```
df_Worldwide_pivot=df_Worldwide.pivot_table(df_Worldwide, index=['country_region','updated'])

df_Worldwide_pivot
```

Python

```
df_Worldwide.plot(kind='line',x='updated',y="confirmed",grid=True)
df_Worldwide.plot(kind='line',x='updated',y="deaths",grid=True)
df_Worldwide.plot(kind='line',x='updated',y="confirmed_change",grid=True)
df_Worldwide.plot(kind='line',x='updated',y="deaths_change",grid=True)
```

Azure Databricks

azure-storage

Sample not available for this platform/package combination.

Azure Synapse

azure-storage

Sample not available for this platform/package combination.

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

COVID Tracking project

Article • 04/19/2022

The COVID Tracking Project dataset provides the latest numbers on tests, confirmed cases, hospitalizations, and patient outcomes from every US state and territory.

For more information about this dataset, see the [project GitHub repository](#).

ⓘ Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Datasets

Modified versions of the dataset are available in CSV, JSON, JSON-Lines, and Parquet.

- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_tracking/latest/covid_tracking.csv
- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_tracking/latest/covid_tracking.json
- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_tracking/latest/covid_tracking.jsonl
- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_tracking/latest/covid_tracking.parquet

All modified versions have ISO 3166 subdivision codes and load times added, and use lower case column names with underscore separators.

Raw data: 'https://pandemicdatalake.blob.core.windows.net/public/raw/covid-19/covid_tracking/latest/daily.json'

Previous versions of modified and raw data: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_tracking/

https://pandemicdatalake.blob.core.windows.net/public/raw/covid-19/covid_tracking/

Data volume

All datasets are updated daily. As of May 13, 2020 they contained 4,100 rows (CSV 574 KB, JSON 1.8 MB, JSONL 1.8 MB, Parquet 334 KB).

Data source

This data is originally published by the COVID Tracking Project at the Atlantic. Raw data is ingested from the COVID Tracking GitHub repo using the [states_daily_4p_et.csv file](#). For more information on this dataset including its origins from the COVID Tracking Project API, see the [project GitHub repository](#).

Data quality

COVID Tracking Project grades the data quality for each state and provides further information about their assessment of the quality of the data. For more information, see the [COVID Tracking Project data page](#). Data in the GitHub repository may be an hour behind the API; use of the API is necessary to access the most recent data.

License and use rights attribution

This data is licensed under the terms and conditions of the [Apache License 2.0](#).

Any use of the data must retain all copyright, patent, trademark, and attribution notices.

Contact

For any questions or feedback about this or other datasets in the COVID-19 Data Lake, contact askcovid19dl@microsoft.com.

Columns

Name	Data type	Unique	Values (sample)	Description
date	date	420	2020-11-10 2021-01-30	Date for which the daily totals were collected.
date_checked	string	9,487	2020-12-01T00:00:00Z 2020-09-01T00:00:00Z	Deprecated
death	smallint	7,327	2 5	Total number of people who have died as a result of COVID-19 so far.
death_increase	smallint	429	1 2	Deprecated
fips	smallint	56	26 55	Census FIPS code for the state.
fips_code	string	60	53 25	Census FIPS code for the state.
hash	string	20,780	63df8cccd23a5476bab2d8111b138e4c9becd35e c606cd6990f16086b5382e12d84f6206172d493d	A hash for this record
hospitalized	int	7,641	89995 4	Deprecated
hospitalized_cumulative	int	7,641	89995 4	Total number of people who have gone to the hospital for COVID-19 so far, including those who have since recovered or died.
hospitalized_currently	smallint	3,886	8 13	Number of people in hospital for COVID-19 on this day.
hospitalized_increase	smallint	615	1 2	Deprecated
in_icu_cumulative	smallint	2,295	990 220	Total number of people who have gone to the ICU for COVID-19 so far, including those who have since recovered or died.
in_icu_currently	smallint	1,643	2 8	Total number of people in the ICU for COVID-19 on this day.
iso_country	string	1	US	ISO 3166 country or region code
iso_subdivision	string	57	US-UM US-WA	ISO 3166 subdivision code
last_update_et	timestamp	9,487	2020-12-01 00:00:00 2020-09-01 00:00:00	Last time the day's data was updated
load_time	timestamp	1	2021-04-26 00:06:49.883000	Date and time the data was loaded to Azure from the source
negative	int	10,864	305972 2140	Total number of people who have tested negative for COVID-19 so far.
negative_increase	int	7,328	6 17	Deprecated
on_ventilator_cumulative	smallint	677	411 412	Total number of people who have used a ventilator for COVID-19 so far, including those who have since recovered or died.
on_ventilator_currently	smallint	837	4 10	Number of people using a ventilator for COVID-19 on this day.
pending	smallint	944	2 17	Number of tests whose results have yet to be determined.
pos_neg	int	18,282	2140 2	Deprecated
positive	int	16,837	2 1	Total number of people who have tested positive for COVID-19 so far.
positive_increase	smallint	4,754	1 2	Deprecated
recovered	int	8,286	29 19	Total number of people who have recovered from COVID-19 so far.
state	string	56	MI PA	Two-letter code for the state.
total	int	18,283	2140 2	Deprecated
total_test_results	int	18,648	2140 3	Total test results provided by the State
total_test_results_increase	int	13,463	1 2	Deprecated

Preview

date	state	positive	hospitalized_currently	hospitalized_cumulative	on_ventilator_currently	data_quality_grade	last_update_et	hash
2021-03-07	AK	56886	33	1293	2	null	3/5/2021 3:59:00 AM	dc4bcccd4bb885
2021-03-07	AL	499819	494	45976		null	3/7/2021 11:00:00 AM	997207b430824
2021-03-07	AR	324818	335	14926	65	null	3/7/2021 12:00:00 AM	50921aeeefba3e3
2021-03-07	AS	0				null	12/1/2020 12:00:00 AM	96d23f888c995f
2021-03-07	AZ	826454	963	57907	143	null	3/7/2021 12:00:00 AM	0437a7a96f4471
2021-03-07	CA	3501394	4291			null	3/7/2021 2:59:00 AM	63c5c0fd2daef2
2021-03-07	CO	436602	326	23904		null	3/7/2021 1:59:00 AM	444746cda3a591
2021-03-07	CT	285330	428	12257		null	3/4/2021 11:59:00 PM	bcc0f7bc8c2bf7
2021-03-07	DC	41419	150		16	null	3/6/2021 12:00:00 AM	a3aa0d623d538
2021-03-07	DE	88354	104			null	3/6/2021 6:00:00 PM	059d870e689d5

Data access

Azure Notebooks

azure-storage

URLs of different dataset file formats hosted on Azure Blob Storage:

CSV: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_tracking/latest/covid_tracking.csv ↗

JSON: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_tracking/latest/covid_tracking.json ↗

JSONL: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_tracking/latest/covid_tracking.jsonl ↗

Parquet: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_tracking/latest/covid_tracking.parquet ↗

Download the dataset file using the built-in capability download from an http URL in Pandas. Pandas has readers for various file formats:

https://pandas.pydata.org/pandas-docs/stable/reference/api/pandas.read_parquet.html ↗

https://pandas.pydata.org/pandas-docs/stable/reference/api/pandas.read_csv.html ↗

Python

```
import pandas as pd
import numpy as np
%matplotlib inline
```

```
import matplotlib.pyplot as plt

df = pd.read_parquet("https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_tracking/latest/covid_tracking.parquet ")
df.head(10)

df.dtypes

df.groupby('state').first().filter(['date', 'positive', 'death'])

df.groupby(df.state).agg({'state': 'count', 'positive_increase': 'sum', 'death_increase': 'sum'})

df_NY=df[df['state'] == 'NY']
df_NY.plot(kind='line',x='date',y="positive",grid=True)
df_NY.plot(kind='line',x='date',y="positive_increase",grid=True)
df_NY.plot(kind='line',x='date',y="death",grid=True)
df_NY.plot(kind='line',x='date',y="death_increase",grid=True)

df_US=df.groupby(df.date).agg({'positive': 'sum','positive_increase': 'sum','death':'sum','death_increase': 'sum'}).reset_index()

df_US.plot(kind='line',x='date',y="positive",grid=True)
df_US.plot(kind='line',x='date',y="positive_increase",grid=True)
df_US.plot(kind='line',x='date',y="death",grid=True)
df_US.plot(kind='line',x='date',y="death_increase",grid=True)
```

Azure Databricks

azure-storage

Sample not available for this platform/package combination.

Azure Synapse

azure-storage

Sample not available for this platform/package combination.

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

European Centre for Disease Prevention and Control (ECDC) COVID-19 Cases

Article • 04/19/2022

The [latest available public data](#) on geographic distribution of COVID-19 cases worldwide from the European Center for Disease Prevention and Control (ECDC). Each row/entry contains the number of new cases reported per day and per country or region.

ⓘ Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Datasets

Modified versions of the dataset are available in CSV, JSON, JSON-Lines, and Parquet, updated daily:

- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/ecdc_cases/latest/ecdc_cases.csv
- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/ecdc_cases/latest/ecdc_cases.json
- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/ecdc_cases/latest/ecdc_cases.jsonl
- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/ecdc_cases/latest/ecdc_cases.parquet

All modified versions have iso_country_region codes and load times added, and use lower case column names with underscore separators.

Raw data: https://pandemicdatalake.blob.core.windows.net/public/raw/covid-19/ecdc_cases/latest/ECDCases.csv

Previous versions of modified and raw data: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/ecdc_cases/ https://pandemicdatalake.blob.core.windows.net/public/raw/covid-19/ecdc_cases/

Data volume

As of May 28, 2020 they contained 19,876 rows (CSV 1.5 MB, JSON 4.9 MB, JSONL 4.9 MB, Parquet 54.1 KB).

Data source

Raw data is ingested daily from the [ECDC csv file](#). For more information on this dataset, including its origins, see the [ECDC data collection page](#).

Data quality

The ECDC does not guarantee the accuracy or timeliness of the data. [Read the disclaimer](#).

License and use rights attribution

This data is made available and may be used as permitted under the ECDC copyright policy here. For any documents where the copyright lies with a third party, permission for reproduction must be obtained from the copyright holder.

ECDC must always be acknowledged as the original source of this data. Such acknowledgment must be included in each copy of the material.

Contact

For any questions or feedback about this or other datasets in the COVID-19 Data Lake, please contact askcovid19dl@microsoft.com.

Columns

Name	Data type	Unique	Values (sample)	Description
cases	smallint	5,515	1 2	Number of reported cases
continent_exp	string	6	Europe Africa	Continent name
countries_and_territories	string	214	Canada Belgium	Country or territory name
country_territory_code	string	213	KOR ISL	Three letter country or territory code
date_rep	date	350	2020-12-11 2020-11-22	Date of the report
day	smallint	31	14 13	Day of month
deaths	smallint	1,049	1 2	Number of reported deaths
geo_id	string	214	CA SE	Geo identifier
iso_country	string	214	SE US	ISO 3166 country or region code
load_date	timestamp	1	2021-04-26 00:06:22.123000	Date the data was loaded to Azure
month	smallint	12	10 8	Month number
year	smallint	2	2020 2019	Year

Preview

date_rep	day	month	year	cases	deaths	countries_and_territories	geo_id	country_territory_code	continent_exp	load_date	iso_country
2020-12-14	14	12	2020	746	6	Afghanistan	AF	AFG	Asia	4/26/2021 12:06:22 AM	AF
2020-12-13	13	12	2020	298	9	Afghanistan	AF	AFG	Asia	4/26/2021 12:06:22 AM	AF
2020-12-12	12	12	2020	113	11	Afghanistan	AF	AFG	Asia	4/26/2021 12:06:22 AM	AF
2020-12-11	11	12	2020	63	10	Afghanistan	AF	AFG	Asia	4/26/2021 12:06:22 AM	AF
2020-12-10	10	12	2020	202	16	Afghanistan	AF	AFG	Asia	4/26/2021 12:06:22 AM	AF
2020-12-09	9	12	2020	135	13	Afghanistan	AF	AFG	Asia	4/26/2021 12:06:22 AM	AF
2020-12-08	8	12	2020	200	6	Afghanistan	AF	AFG	Asia	4/26/2021 12:06:22 AM	AF
2020-12-07	7	12	2020	210	26	Afghanistan	AF	AFG	Asia	4/26/2021 12:06:22 AM	AF
2020-12-06	6	12	2020	234	10	Afghanistan	AF	AFG	Asia	4/26/2021 12:06:22 AM	AF
2020-12-05	5	12	2020	235	18	Afghanistan	AF	AFG	Asia	4/26/2021 12:06:22 AM	AF

Data access

Azure Notebooks

azure-storage

This notebook documents the URLs and sample code to access the European Centre for Disease Prevention and Control (ECDC) Covid-19 Cases dataset URLs of different dataset file formats hosted on Azure Blob Storage:
CSV:

https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/ecdc_cases/latest/ecdc_cases.csv ↗

JSON: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/ecdc_cases/latest/ecdc_cases.json ↗

JSONL: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/ecdc_cases/latest/ecdc_cases.jsonl ↗

Parquet: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/ecdc_cases/latest/ecdc_cases.parquet ↗

Download the dataset file using the built-in capability download from an http URL in Pandas. Pandas has readers for various file formats:

https://pandas.pydata.org/pandas-docs/stable/reference/api/pandas.read_parquet.html ↗

https://pandas.pydata.org/pandas-docs/stable/reference/api/pandas.read_csv.html ↗

Python

```
import pandas as pd
import numpy as np
%matplotlib inline
import matplotlib.pyplot as plt

df = pd.read_parquet("https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/ecdc_cases/latest/ecdc_cases.parquet")
df.head(10)

df.dtypes

df.groupby('countries_and_territories').first().filter(['continent_exp','cases', 'deaths','date_rep'])

df.groupby('continent_exp').agg({'countries_and_territories': 'count','cases': 'count','deaths': 'count'})

import plotly.graph_objects as go
import plotly.express as px
import matplotlib.pyplot as plt

df.loc[:, ['countries_and_territories', 'cases', 'deaths']].groupby(['countries_and_territories']).max().sort_values(by='cases',ascending=False).reset_index()
[:15].style.background_gradient(cmap='rainbow')

df_Worldwide=df[df['countries_and_territories']=='United_States_of_America']

df.plot(kind='line',x='date_rep',y="cases",grid=True)
df.plot(kind='line',x='date_rep',y="deaths",grid=True)
#df_Worldwide.plot(kind='line',x='date_rep',y="confirmed_change",grid=True)
#df_Worldwide.plot(kind='line',x='date_rep',y="deaths_change",grid=True)
```

Azure Databricks

azure-storage

Sample not available for this platform/package combination.

Azure Synapse

azure-storage

Sample not available for this platform/package combination.

Examples

See examples of how this dataset can be used:

- [Analyze COVID data with Synapse SQL serverless endpoint ↗](#)
- [Linear regression analysis on COVID data using SQL endpoint in Azure Synapse Analytics ↗](#)

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

Oxford COVID-19 Government Response Tracker

Article • 09/07/2022

The [Oxford Covid-19 Government Response Tracker \(OxCGRT\) dataset](#) contains systematic information on which governments have taken which measures, and when.

This information can help decision-makers and citizens understand governmental responses in a consistent way, aiding efforts to fight the pandemic. The OxCGRT systematically collects information on several different common policy responses governments have taken, records these policies on a scale to reflect the extent of government action, and aggregates these scores into a suite of policy indices.

ⓘ Note

Microsoft provides Azure Open Datasets on an “as is” basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Datasets

Modified versions of the dataset are available in CSV, JSON, JSON-Lines, and Parquet, updated daily:

- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_policy_tracker/latest/covid_policy_tracker.csv
- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_policy_tracker/latest/covid_policy_tracker.json
- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_policy_tracker/latest/covid_policy_tracker.jsonl
- https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_policy_tracker/latest/covid_policy_tracker.parquet

All modified versions have iso_country codes and load times added, and use lower case column names with underscore separators.

Raw data: https://pandemicdatalake.blob.core.windows.net/public/raw/covid-19/covid_policy_tracker/latest/CovidPolicyTracker.csv

Previous versions of modified and raw data: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_policy_tracker/ https://pandemicdatalake.blob.core.windows.net/public/raw/covid-19/covid_policy_tracker/

Data volume

As of June 8, 2020 they contained 27,919 rows (CSV 4.9 MB, JSON 20.9 MB, JSONL 20.8 MB, Parquet 133.0 KB).

Data source

The source of this data is Thomas Hale, Sam Webster, Anna Petherick, Toby Phillips, and Beatriz Kira. (2020). Oxford COVID-19 Government Response Tracker. [Blavatnik School of Government](#). Raw data is ingested daily from the [latest OxCGRT csv file](#). For more information on this dataset, including how it is collected, see the [Government tracker response site](#).

Data quality

The OxCGRT does not guarantee the accuracy or timeliness of the data. For more information, see the [data quality statement](#).

License and use rights attribution

This data is licensed under the [Creative Commons Attribution 4.0 International License](#).

Cite as: Thomas Hale, Sam Webster, Anna Petherick, Toby Phillips, and Beatriz Kira. (2020). Oxford COVID-19 Government Response Tracker. Blavatnik School of Government.

Contact

For any questions or feedback about this or other datasets in the COVID-19 Data Lake, contact askcovid19dl@microsoft.com.

Columns

Name	Data type	Unique	Values (sample)	Description
c1_flag	boolean	3	True	Binary flag for geographic scope. 0 - targeted 1 - general Blank - no data
c1_school_closing	double	5	3.0 2.0	Record closings of schools and universities. 0 - no measures 1 - recommend closing 2 - require closing (only some levels or categories, for example, just high school, or just public schools) 3 - require closing all levels Blank - no data
c2_flag	boolean	3	True	Binary flag for geographic scope. 0 - targeted; 1 - general; Blank - no data
c2_workplace_closing	double	5	2.0 1.0	Record closings of workplaces. 0 - no measures 1 - recommend closing (or recommend work from home) 2 - require closing (or work from home) for some sectors or categories of workers 3 - require closing (or work from home) for all-but-essential workplaces (for example, grocery stores, doctors) Blank - no data
c3_cancel_public_events	double	4	2.0 1.0	Record canceling public events. 0 - no measures 1 - recommend canceling 2 - require canceling Blank - no data
c3_flag	boolean	3	True	Binary flag for geographic scope. 0 - targeted 1 - general Blank - no data
c4_flag	boolean	3	True	Binary flag for geographic scope 0 - targeted 1 - general Blank - no data
c4_restrictions_on_gatherings	double	6	4.0 3.0	Record limits on private gatherings. 0 - no restrictions 1 - restrictions on very large gatherings (the limit is above 1000 people) 2 - restrictions on gatherings between 101-1000 people 3 - restrictions on gatherings between 11-100 people 4 - restrictions on gatherings of 10 people or less Blank - no data
c5_close_public_transport	double	4	1.0 2.0	Record closing of public transport 0 - no measures 1 - recommend closing (or significantly reduce volume/route/means of transport available) 2 - require closing (or prohibit most citizens from using it) Blank - no data
c5_flag	boolean	3	True	Binary flag for geographic scope 0 - targeted 1 - general Blank - no data
c6_flag	boolean	3	True	Binary flag for geographic scope 0 - targeted 1 - general Blank - no data
c6_stay_at_home_requirements	double	5	1.0 2.0	Record orders to "shelter-in-place" and otherwise confine to the home 0 - no measures 1 - recommend not leaving house 2 - require not leaving house with exceptions for daily exercise, grocery shopping, and 'essential' trips 3 - require not leaving house with minimal exceptions (for example, allowed to leave once a week, or only one person can leave at a time, etc.) Blank - no data
c7_flag	boolean	3	True	Binary flag for geographic scope 0 - targeted 1 - general Blank - no data
c7_restrictions_on_internal_movement	double	4	2.0 1.0	Record restrictions on internal movement between cities/regions 0 - no measures 1 - recommend not to travel between regions/cities 2 - internal movement restrictions in place Blank - no data
c8_international_travel_controls	double	6	3.0 4.0	Record restrictions on international travel. Note: this records policy for foreign travelers, not citizens 0 - no restrictions 1 - screening arrivals 2 - quarantine arrivals from some or all regions 3 - ban arrivals from some regions 4 - ban on all regions or total border closure Blank - no data
confirmedcases	smallint	18,238	1 2	
confirmeddeaths	smallint	14,906	1 2	
countrycode	string	186	USA BRA	
countryname	string	186	United States Brazil	

Name	Data type	Unique	Values (sample)	Description
date	date	478	2020-08-25 2021-03-30	
e1_flag	boolean	3	True	Binary flag for sectoral scope 0 - formal sector workers only 1 - transfers to informal sector workers to Blank - no data
e1_income_support	double	4	1.0 2.0	Record if the government is providing direct cash payments to people who lose their jobs or cannot work. Note: only includes payments to firms if explicitly linked to payroll/salaries 0 - no income support 1 - government is replacing less than 50% of lost salary (or if a flat sum, it is less than 50% median salary) 2 - government is replacing 50% or more of lost salary (or if a flat sum, it is greater than 50% median salary) Blank - no data
e2_debt/contract_relief	double	4	1.0 2.0	
e3_fiscal_measures	double	819	-0.01 3.0	Announced economic stimulus spending Note: only record amount additional to previously announced spending Record monetary value in USD of fiscal stimuli, includes any spending or tax cuts NOT included in E4, H4, or H5 0 - no new spending that day Blank - no data
e4_international_support	double	113	-0.02 5000000.0	Announced offers of Covid-19-related aid spending to other countries/regions Note: only record amount additional to previously announced spending Record monetary value in USD 0 - no new spending that day Blank - no data
h1_flag	boolean	3	True	Binary flag for geographic scope 0 - targeted 1 - general Blank - no data
h1_public_information_campaigns	double	4	2.0 1.0	Record presence of public info campaigns 0 - no Covid-19 public information campaign 1 - public officials urging caution about Covid-19 2- coordinated public information campaign (for example, across traditional and social media) Blank - no data
h2_testing_policy	double	5	2.0 1.0	Record government policy on who has access to testing Note: this records policies about testing for current infection (PCR tests) not testing for immunity (antibody test) 0 - no testing policy 1 - only those who both (a) have symptoms AND (b) meet specific criteria (for example, key workers, admitted to hospital, came into contact with a known case, returned from overseas) 2 - testing of anyone showing Covid-19 symptoms 3 - open public testing (for example "drive through" testing available to asymptomatic people) Blank - no data
h3_contact_tracing	double	4	2.0 1.0	Record government policy on contact tracing after a positive diagnosis Note: we are looking for policies that would identify all people potentially exposed to Covid-19; voluntary bluetooth apps are unlikely to achieve this 0 - no contact tracing 1 - limited contact tracing; not done for all cases 2 - comprehensive contact tracing; done for all identified cases
h4_emergency_investment_in_healthcare	double	462	35.0 562.0	Announced short-term spending on healthcare system, for example, hospitals, masks, etc. Note: only record amount additional to previously announced spending Record monetary value in USD 0 - no new spending that day Blank - no data
h5_investment_in_vaccines	double	133	1.0 191.0	Announced public spending on Covid-19 vaccine development Note: only record amount additional to previously announced spending Record monetary value in USD 0 - no new spending that day Blank - no data
iso_country	string	186	US BR	ISO 3166 country or region code
load_date	timestamp	1	2021-04-26 00:06:25.157000	Date and time data was loaded from external source
stringencyindex	double	188	11.11 60.19	
stringencyindexfordisplay	double	188	11.11 60.19	

Preview

countryname	countrycode	date	c1_school_closing	c2_workplace_closing	c3_cancel_public_events	c4_restrictions_on_gatherings	c5_close_public
-------------	-------------	------	-------------------	----------------------	-------------------------	-------------------------------	-----------------

countryname	countrycode	date	c1_school_closing	c2_workplace_closing	c3_cancel_public_events	c4_restrictions_on_gatherings	c5_close_public
Aruba	ABW	2020-01-01	0	0	0	0	0
Aruba	ABW	2020-01-02	0	0	0	0	0
Aruba	ABW	2020-01-03	0	0	0	0	0
Aruba	ABW	2020-01-04	0	0	0	0	0
Aruba	ABW	2020-01-05	0	0	0	0	0
Aruba	ABW	2020-01-06	0	0	0	0	0
Aruba	ABW	2020-01-07	0	0	0	0	0
Aruba	ABW	2020-01-08	0	0	0	0	0
Aruba	ABW	2020-01-09	0	0	0	0	0
Aruba	ABW	2020-01-10	0	0	0	0	0

Data access

Azure Notebooks

azure-storage

💡 Tip

Download the notebook instead [↗](#).

This notebook documents the URLs and sample code to access the Oxford Covid-19 Government Response Tracker (OxCGRT) dataset

URLs of different file formats hosted on Azure Blob Storage:

CSV: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_policy_tracker/latest/covid_policy_tracker.csv ↗

JSON: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_policy_tracker/latest/covid_policy_tracker.json ↗

JSONL: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_policy_tracker/latest/covid_policy_tracker.jsonl ↗

Parquet: https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_policy_tracker/latest/covid_policy_tracker.parquet ↗

Download the dataset file using the built-in capability download from an http URL in Pandas. Pandas has readers for various file formats:

https://pandas.pydata.org/pandas-docs/stable/reference/api/pandas.read_parquet.html

https://pandas.pydata.org/pandas-docs/stable/reference/api/pandas.read_csv.html

Start by loading the dataset file into a pandas dataframe and view some sample rows

Python

```
import pandas as pd
import numpy as np
%matplotlib inline
import matplotlib.pyplot as plt

df = pd.read_parquet("https://pandemicdatalake.blob.core.windows.net/public/curated/covid-19/covid_policy_tracker/latest/covid_policy_tracker.parquet")
df.head(10)
```

Lets check the data types of the various fields and verify that the updated column is datetime format

Python

```
df.dtypes
```

This dataset contains data for the numerous countries/regions. Lets verify what countries/regions we have data for.

We will start by looking at the latest data for each country:

Python

```
df.groupby('countryname').first().filter(['confirmedcases', 'confirmeddeaths', 'h5_investment_in_vaccines',
                                         'c6_stay_at_home_requirements', 'h4_emergency_investment_in_healthcare', 'c4_restrictions_on_gatherings',
                                         'load_date'])
```

Next, we will do some aggregations to make sure columns such as `confirmedcases` and `confirmeddeaths` tally with the latest data. You should see that positive and death numbers for latest date in the above table match with the aggregation of `confirmedcases` and `confirmeddeaths`.

Python

```
df.groupby('countryname').agg({'countryname': 'count', 'confirmedcases': 'sum', 'confirmeddeaths': 'sum',
                               'h5_investment_in_vaccines': 'count', 'c6_stay_at_home_requirements': 'sum'})
```

Lets do some basic visualizations for a few countries/regions

Python

```
import plotly.graph_objects as go
import plotly.express as px
import matplotlib.pyplot as plt

df.loc[:, ['countryname', 'confirmedcases', 'confirmeddeaths']].groupby(['countryname']).max().sort_values(by='confirmedcases',
                                                                                                         ascending=False).reset_index()
[:15].style.background_gradient(cmap='rainbow')
```

Python

```
df_US = df.groupby(df.date).agg({'confirmedcases': 'sum', 'confirmeddeaths': 'sum'}).reset_index()

df_US.plot(kind='line', x='date', y="confirmedcases", grid=True)
df_US.plot(kind='line', x='date', y="confirmeddeaths", grid=True)
```

azure-storage

Sample not available for this platform/package combination.

Azure Synapse

azure-storage

Sample not available for this platform/package combination.

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

COVID-19 Open Research Dataset

Article • 04/19/2022

Full-text and metadata dataset of COVID-19 and coronavirus-related scholarly articles optimized for machine readability and made available for use by the global research community.

In response to the COVID-19 pandemic, the [Allen Institute for AI](#) has partnered with leading research groups to prepare and distribute the COVID-19 Open Research Dataset (CORD-19). This dataset is a free resource of over 47,000 scholarly articles, including over 36,000 with full text, about COVID-19 and the coronavirus family of viruses for use by the global research community.

This dataset mobilizes researchers to apply recent advances in natural language processing to generate new insights in support of the fight against this infectious disease.

The corpus may be updated as new research is published in peer-reviewed publications and archival services like [bioRxiv](#), [medRxiv](#), and others.

Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

License Terms

This dataset is made available by the Allen Institute of AI and [Semantic Scholar](#). By accessing, downloading, or otherwise using any content provided in the CORD-19 Dataset, you agree to the [Dataset License](#) related to the use this dataset. Specific licensing information for individual articles in the dataset is available in the metadata file. More licensing information is available on the [PMC website](#), [medRxiv website](#), and [bioRxiv website](#).

Volume and retention

This dataset is stored in JSON format and the latest release contains over 36,000 full text articles. Each paper is represented as a single JSON object. [View the schema ↗](#).

Storage Location

This dataset is stored in the East US Azure region. Locating compute resources in East US is recommended for affinity.

Citation

When including CORD-19 data in a publication or redistribution, cite the dataset as follows:

In bibliography:

COVID-19 Open Research Dataset (CORD-19). 2020. Version YYYY-MM-DD. Retrieved from [COVID-19 Open Research Dataset \(CORD-19\) ↗](#). Accessed YYYY-MM-DD. doi:10.5281/zenodo.3715505

In text: (CORD-19, 2020)

Contact

For questions about this dataset, contact partnerships@allenai.org.

Data access

Azure Notebooks

azure-storage

💡 Tip

[Download the notebook instead ↗](#).

The CORD-19 Dataset

CORD-19 is a collection of over 50,000 scholarly articles - including over 40,000 with full text - about COVID-19, SARS-CoV-2, and related corona viruses. This dataset has been made freely available with the goal to aid research communities combat the COVID-19 pandemic.

The goal of this notebook is two-fold:

1. Demonstrate how to access the CORD-19 dataset on Azure: We connect to the Azure blob storage account housing the CORD-19 dataset.
2. Walk though the structure of the dataset: Articles in the dataset are stored as json files. We provide examples showing:
 - How to find the articles (navigating the container)
 - How to read the articles (navigating the json schema)

Dependencies: This notebook requires the following libraries:

- Azure storage (for example, `pip install azure-storage`)
- NLTK ([docs](#))
- Pandas (for example, `pip install pandas`)

Getting the CORD-19 data from Azure

The CORD-19 data has been uploaded as an Azure Open Dataset [here](#). We create a blob service linked to this CORD-19 open dataset.

Python

```
from azure.storage.blob import BlockBlobService

# storage account details
azure_storage_account_name = "azureopendatastorage"
azure_storage_sas_token = "sv=2019-02-
02&ss=bfqt&srt=sco&sp=rlcup&se=2025-04-14T00:21:16Z&st=2020-04-
13T16:21:16Z&spr=https&sig=JgwLYbdGruHxRYTpr5dxfJqobKbhGap8WUtKFadcivQ%3
D"

# create a blob service
blob_service = BlockBlobService(
    account_name=azure_storage_account_name,
    sas_token=azure_storage_sas_token,
)
```

We can use this blob service as a handle on the data. We can navigate the dataset making use of the `BlockBlobService` APIs. See [here](#) for more details:

- [Blob service concepts](#)
- [Operations on containers](#)

The CORD-19 data is stored in the `covid19temp` container. This is the file structure within the container together with an example file.

```
metadata.csv
custom_license/
    pdf_json/
        0001418189999fea7f7cbe3e82703d71c85a6fe5.json      # filename
is sha-hash
    ...
    pmc_json/
        PMC1065028.xml.json                                # filename
is the PMC ID
    ...
noncomm_use_subset/
    pdf_json/
        0036b28fddf7e93da0970303672934ea2f9944e7.json
    ...
    pmc_json/
        PMC1616946.xml.json
    ...
comm_use_subset/
    pdf_json/
        000b7d1517ceebb34e1e3e817695b6de03e2fa78.json
    ...
    pmc_json/
        PMC1054884.xml.json
    ...
biorxiv_medrxiv/                                # note:
there is no pmc_json subdir
    pdf_json/
        0015023cc06b5362d332b3baf348d11567ca2fbb.json
    ...
```

Each .json file corresponds to an individual article in the dataset. This is where the title, authors, abstract and (where available) the full text data is stored.

Using `metadata.csv`

The CORD-19 dataset comes with `metadata.csv` - a single file that records basic information on all the papers available in the CORD-19 dataset. This is a good place to start exploring!

Python

```
# container housing CORD-19 data
container_name = "covid19temp"

# download metadata.csv
metadata_filename = 'metadata.csv'
blob_service.get_blob_to_path(
    container_name=container_name,
    blob_name=metadata_filename,
    file_path=metadata_filename
)
```

Python

```
import pandas as pd

# read metadata.csv into a dataframe
metadata_filename = 'metadata.csv'
metadata = pd.read_csv(metadata_filename)
```

Python

```
metadata.head(3)
```

That's a lot to take in at first glance, so let's apply a little polish.

Python

```
simple_schema = ['cord_uid', 'source_x', 'title', 'abstract', 'authors',
'full_text_file', 'url']

def make_clickable(address):
    '''Make the url clickable'''
    return '<a href="{0}">{0}</a>'.format(address)

def preview(text):
    '''Show only a preview of the text data.'''
    return text[:30] + '...'

format_ = {'title': preview, 'abstract': preview, 'authors': preview,
'url': make_clickable}

metadata[simple_schema].head().style.format(format_)
```

Python

```
# let's take a quick look around
num_entries = len(metadata)
print("There are {} many entries in this dataset:".format(num_entries))
```

```

metadata_with_text = metadata[metadata['full_text_file'].isna() == False]
with_full_text = len(metadata_with_text)
print("-- {} have full text entries".format(with_full_text))

with_doi = metadata['doi'].count()
print("-- {} have DOIs".format(with_doi))

with_pmcid = metadata['pmcid'].count()
print("-- {} have PubMed Central (PMC) ids".format(with_pmcid))

with_microsoft_id = metadata['Microsoft Academic Paper ID'].count()
print("-- {} have Microsoft Academic paper ids".format(with_microsoft_id))

```

There are 51078 many entries in this dataset:

```

-- 42511 have full text entries
-- 47741 have DOIs
-- 41082 have PubMed Central (PMC) ids
-- 964 have Microsoft Academic paper ids

```

Example: Read full text

`metadata.csv` doesn't contain the full-text itself. Let's see an example of how to read that. Locate and unpack the full text json and convert it to a list of sentences.

Python

```

# choose a random example with pdf parse available
metadata_with_pdf_parse = metadata[metadata['has_pdf_parse']]
example_entry = metadata_with_pdf_parse.iloc[42]

# construct path to blob containing full text
blob_name =
'{0}/pdf_json/{1}.json'.format(example_entry['full_text_file'],
example_entry['sha']) # note the repetition in the path
print("Full text blob for this entry:")
print(blob_name)

```

We can now read the json content associated to this blob as follows.

Python

```

import json
blob_as_json_string =

```

```

blob_service.get_blob_to_text(container_name=container_name,
blob_name=blob_name)
data = json.loads(blob_as_json_string.content)

# in addition to the body text, the metadata is also stored within the
# individual json files
print("Keys within data:", ', '.join(data.keys()))

```

For the purposes of this example, we are interested in the `body_text`, which stores the text data as follows:

JSON

```

"body_text": [                                # list of paragraphs in full body
  {
    "text": <str>,                          # list of character indices of
    "cite_spans": [                         # e.g. citation "[7]" occurs at
      inline citations                      # linked to bibliography entry
      positions 151-154 in "text"
    ],
    "ref_spans": <list of dicts similar to cite_spans>,      # e.g.
    inline reference to "Table 1"
    "section": "Abstract"
  },
  ...
]

```

The full json schema is available [here](#).

Python

```

from nltk.tokenize import sent_tokenize

# the text itself lives under 'body_text'
text = data['body_text']

# many NLP tasks play nicely with a list of sentences
sentences = []
for paragraph in text:
    sentences.extend(sent_tokenize(paragraph['text']))

```

```
print("An example sentence:", sentences[0])
```

PDF vs PMC XML Parse

In the above example, we looked at a case with `has_pdf_parse == True`. In that case the blob file path was of the form:

```
'<full_text_file>/pdf_json/<sha>.json'
```

Alternatively, for cases with `has_pmc_xml_parse == True` use the following format:

```
'<full_text_file>/pmc_json/<pmcid>.xml.json'
```

For example:

Python

```
# choose a random example with pmc parse available
metadata_with_pmc_parse = metadata[metadata['has_pmc_xml_parse']]
example_entry = metadata_with_pmc_parse.iloc[42]

# construct path to blob containing full text
blob_name =
'{0}/pmc_json/{1}.xml.json'.format(example_entry['full_text_file'],
example_entry['pmcid']) # note the repetition in the path
print("Full text blob for this entry:")
print(blob_name)

blob_as_json_string =
blob_service.get_blob_to_text(container_name=container_name,
blob_name=blob_name)
data = json.loads(blob_as_json_string.content)

# the text itself lives under 'body_text'
text = data['body_text']

# many NLP tasks play nicely with a list of sentences
sentences = []
for paragraph in text:
    sentences.extend(sent_tokenize(paragraph['text']))

print("An example sentence:", sentences[0])
```

Full text blob for this entry:
custom_license/pmc_json/PMC546170.xml.json
An example sentence: Double-stranded small interfering RNA (siRNA) molecules have drawn much attention since it was unambiguously shown that they mediate potent gene knock-down in a variety of mammalian cells (1).

Iterate through blobs directly

In the above examples, we used the `metadata.csv` file to navigate the data, construct the blob file path, and read data from the blob. An alternative is to iterate through the blobs themselves.

Python

```
# get and sort list of available blobs
blobs = blob_service.list_blobs(container_name)
sorted_blobs = sorted(list(blobs), key=lambda e: e.name, reverse=True)
```

Now we can iterate through the blobs directly. For example, let's count the number json files available.

Python

```
# we can now iterate directly though the blobs
count = 0
for blob in sorted_blobs:
    if blob.name[-5:] == ".json":
        count += 1
print("There are {} many json files".format(count))
```

There are 59784 many json files

Appendix

Data quality issues

This is a large dataset that, for obvious reasons, was put together rather hastily! Here are some data quality issues we've observed.

Multiple shas

We observe that in some cases there are multiple shas for a given entry.

Python

```
metadata_multiple_shas = metadata[metadata['sha'].str.len() > 40]

print("There are {} many entries with multiple
shas".format(len(metadata_multiple_shas)))

metadata_multiple_shas.head(3)
```

```
There are 1999 many entries with multiple shas
```

Layout of the container

Here we use a simple regex to explore the file structure of the container in case this is updated in the future.

Python

```
container_name = "covid19temp"
blobs = blob_service.list_blobs(container_name)
sorted_blobs = sorted(list(blobs), key=lambda e: e.name, reverse=True)
```

Python

```
import re
dirs = {}

pattern = '([\w]+)\/([\w]+)\/([\w.]+).json'
for blob in sorted_blobs:

    m = re.match(pattern, blob.name)

    if m:
        dir_ = m[1] + '/' + m[2]

        if dir_ in dirs:
            dirs[dir_] += 1
```

```
    else:  
        dirs[dir_] = 1  
  
dirs
```

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

Diabetes dataset

Article • 04/19/2022

The Diabetes dataset has 442 samples with 10 features, making it ideal for getting started with machine learning algorithms. It's one of the most popular [Scikit Learn Toy Datasets](#).

[Original dataset description](#) | [Original data file](#)

ⓘ Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Columns

Name	Data type	Unique	Values (sample)
AGE	bigint	58	53 60
BMI	double	163	24.1 23.5
BP	double	100	93.0 83.0
S1	bigint	141	162 184
S2	double	302	125.8 114.8
S3	double	63	46.0 38.0
S4	double	66	3.0 4.0
S5	double	184	4.4427 4.3041
S6	bigint	56	92 96
SEX	bigint	2	1 2
Y	bigint	214	72 200

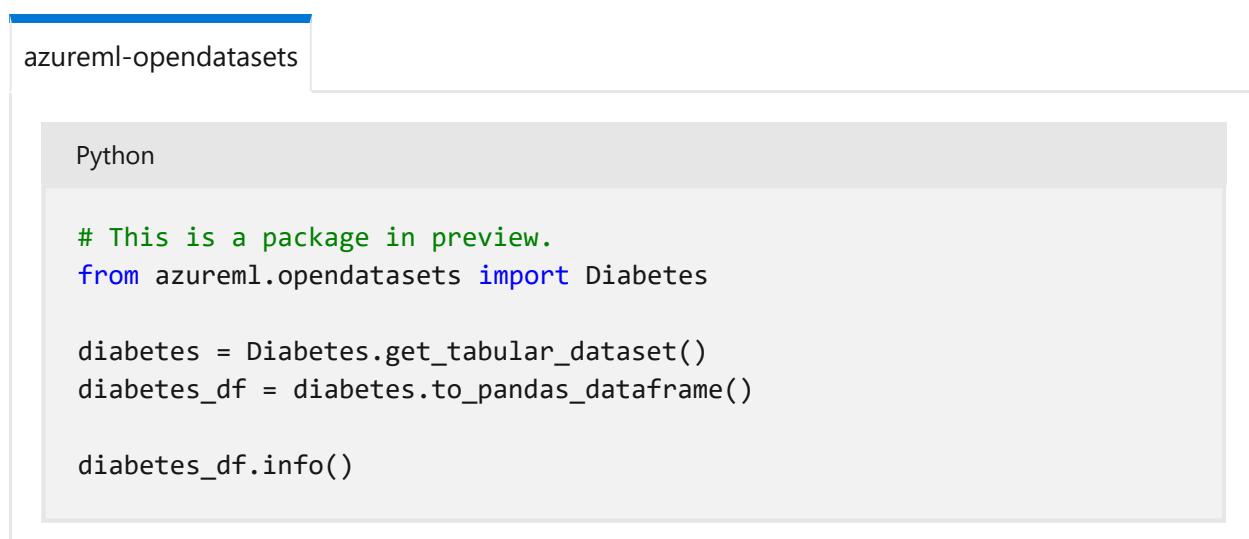
Preview

AGE	SEX	BMI	BP	S1	S2	S3	S4	S5	S6	Y
59	2	32.1	101	157	93.2	38	4	4.8598	87	151
48	1	21.6	87	183	103.2	70	3	3.8918	69	75
72	2	30.5	93	156	93.6	41	4	4.6728	85	141
24	1	25.3	84	198	131.4	40	5	4.8903	89	206
50	1	23	101	192	125.4	52	4	4.2905	80	135
23	1	22.6	89	139	64.8	61	2	4.1897	68	97
36	2	22	90	160	99.6	50	3	3.9512	82	138
66	2	26.2	114	255	185	56	4.55	4.2485	92	63
60	2	32.1	83	179	119.4	42	4	4.4773	94	110
29	1	30	85	180	93.4	43	4	5.3845	88	310

Data access

Use the following code samples to access this dataset in Azure Notebooks, Azure Databricks, or Azure Synapse.

Azure Notebooks



```
azureml-opendatasets
Python

# This is a package in preview.
from azureml.opendatasets import Diabetes

diabetes = Diabetes.get_tabular_dataset()
diabetes_df = diabetes.to_pandas_dataframe()

diabetes_df.info()
```

Azure Databricks

azureml-opendatasets

Python

```
# This is a package in preview.
from azureml.opendatasets import Diabetes

diabetes = Diabetes.get_tabular_dataset()
diabetes_df = diabetes.to_spark_dataframe()

display(diabetes_df.limit(5))
```

Azure Synapse

azureml-opendatasets

Sample not available for this platform/package combination.

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

1000 Genomes

Article • 06/10/2022

The 1000 Genomes Project ran between 2008 and 2015, creating the largest public catalog of human variation and genotype data. The final data set contains data for 2,504 individuals from 26 populations and 84 million identified variants. For more information, see the 1000 Genome Project website and the following publications:

Pilot Analysis: A map of human genome variation from population-scale sequencing
Nature 467, 1061-1073 (28 October 2010)

Phase 1 Analysis: An integrated map of genetic variation from 1,092 human genomes
Nature 491, 56-65 (01 November 2012)

Phase 3 Analysis: A global reference for human genetic variation Nature 526, 68-74 (01 October 2015) and An integrated map of structural variation in 2,504 human genomes
Nature 526, 75-81 (01 October 2015)

For details on data formats refer to <http://www.internationalgenome.org/formats> ↗

[NEW] the dataset is also available in [parquet format](#) ↗

ⓘ Note

Microsoft provides Azure Open Datasets on an “as is” basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Data source

This dataset is a mirror of <ftp://ftp.1000genomes.ebi.ac.uk/vol1/ftp/> ↗

Data volumes and update frequency

This dataset contains approximately 815 TB of data and is updated daily.

Storage location

This dataset is stored in the West US 2 and West Central US Azure regions. Allocating compute resources in West US 2 or West Central US is recommended for affinity.

Data Access

West US 2: '<https://dataset1000genomes.blob.core.windows.net/dataset>'

West Central US: '<https://dataset1000genomes-secondary.blob.core.windows.net/dataset>'

SAS Token: sv=2019-10-

10&si=prod&sr=c&sig=9nzcxaQn0NprMPISh4RhFQHcXedLQlcFgbERiooHEqM%3D

Data Access: Curated 1000 genomes dataset in parquet format

East US: <https://curated1000genomes.blob.core.windows.net/dataset>

SAS Token: sv=2018-03-

28&si=prod&sr=c&sig=BglomQanB355O4FhxqBL9xUgKzwpcVIRZdBewO5%2FM4E%3D

Use Terms

Following the final publications, data from the 1000 Genomes Project is publicly available without embargo to anyone for use under the terms provided by the dataset source (<http://www.internationalgenome.org/data>). Use of the data should be cited per details available in the [FAQs](#) from the 1000 Genome Project.

Contact

<https://www.internationalgenome.org/contact>

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

ClinVar Annotations

Article • 04/19/2022

[ClinVar](#) is a freely accessible, public archive of reports of the relationships among human variations and phenotypes, with supporting evidence. It facilitates access to and communication about the relationships asserted between human variation and observed health status, and the history of that interpretation. It provides access to a broader set of clinical interpretations that can be incorporated into genomics workflows and applications.

For more information on the data, see the [Data Dictionary](#) and [FAQ](#).

ⓘ Note

Microsoft provides Azure Open Datasets on an “as is” basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Data source

This dataset is a mirror of <ftp://ftp.ncbi.nlm.nih.gov/pub/clinvar/xml/>

Data volumes and update frequency

This dataset contains approximately 56 GB of data and is updated daily.

Storage location

This dataset is stored in the West US 2 and West Central US Azure regions. Allocating compute resources in West US 2 or West Central US is recommended for affinity.

Data Access

West US 2: 'https://datasetclinvar.blob.core.windows.net/dataset'

West Central US: 'https://datasetclinvar-secondary.blob.core.windows.net/dataset'

SAS Token: sv=2019-02-02&se=2050-01-

01T08%3A00%3A00Z&si=prod&sr=c&sig=qFPPwPba1RmBvaffkzkLuzabYU5dZstSTgMwxuLNME8%3D

Use Terms

Data is available without restrictions. More information and citation details, see [Accessing and using data in ClinVar](#).

Contact

For any questions or feedback about this dataset, contact clinvar@ncbi.nlm.nih.gov.

Data access

Azure Notebooks

azure-storage

💡 Tip

[Download the notebook instead](#).

Getting the ClinVar data from Azure Open Dataset

Several public genomics data has been uploaded as an Azure Open Dataset [here](#). We create a blob service linked to this open dataset. You can find examples of data calling procedure from Azure Open Dataset for `ClinVar` dataset in below:

Users can call and download the following path with this notebook:

'https://datasetclinvar.blob.core.windows.net/dataset/ClinVarFullRelease_00-latest.xml.gz.md5'

➊ Note

Users needs to log-in their Azure Account via Azure CLI for viewing the data with Azure ML SDK. On the other hand, they do not need do any actions for downloading the data.

For more information on installing the Azure CLI, see [Install the Azure CLI](#)

Calling the data from 'ClinVar Data Set'

Python

```
import azureml.core
print("Azure ML SDK Version: ", azureml.core.VERSION)
```

Python

```
from azureml.core import Dataset
reference_dataset =
Dataset.File.from_files('https://datasetclinvar.blob.core.windows.net/dataset')
mount = reference_dataset.mount()
```

Python

```
import os

REF_DIR = '/dataset'
path = mount.mount_point + REF_DIR

with mount:
    print(os.listdir(path))
```

Python

```
import pandas as pd

# create mount context
mount.start()

# specify path to README file
REF_DIR = '/dataset'
metadata_filename = '{}/{}{}'.format(mount.mount_point, REF_DIR,
'_README')

# read README file
```

```
metadata = pd.read_table(metadata_filename)
metadata
```

Download the specific file

Python

```
import os
import uuid
import sys
from azure.storage.blob import BlockBlobService, PublicAccess

blob_service_client = BlockBlobService(account_name='datasetclinvar',
sas_token='sv=2019-02-02&se=2050-01-
01T08%3A00%3A00Z&si=prod&sr=c&sig=qFPPwPba1RmBvaffkzkLuzabYU5dZstSTgMwxu
LNME8%3D')
blob_service_client.get_blob_to_path('dataset', 'ClinVarFullRelease_00-
latest.xml.gz.md5', './ClinVarFullRelease_00-latest.xml.gz.md5')
```

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

ENCODE: Encyclopedia of DNA Elements

Article • 04/19/2022

The [Encyclopedia of DNA Elements \(ENCODE\) Consortium](#) is an ongoing international collaboration of research groups funded by the National Human Genome Research Institute (NHGRI). ENCODE's goal is to build a comprehensive parts list of functional elements in the human genome, including elements that act at the protein and RNA levels, and regulatory elements that control cells and circumstances in which a gene is active.

ENCODE investigators employ various assays and methods to identify functional elements. The discovery and annotation of gene elements is accomplished primarily by sequencing a diverse range of RNA sources, comparative genomics, integrative bioinformatic methods, and human curation. Regulatory elements are typically investigated through DNA hypersensitivity assays, assays of DNA methylation, and immunoprecipitation (IP) of proteins that interact with DNA and RNA, that is, modified histones, transcription factors, chromatin regulators, and RNA-binding proteins, followed by sequencing.

Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Data source

This dataset is a mirror of the data store at <https://www.encodeproject.org/>

Data volumes and update frequency

This dataset includes approximately 756 TB of data, and is updated monthly during the first week of every month.

Storage location

This dataset is stored in the West US 2 and West Central US Azure regions. We recommend locating compute resources in West US 2 or West Central US for affinity.

Data Access

West US 2: '<https://datasetencode.blob.core.windows.net/dataset>'

West Central US: '<https://datasetencode-secondary.blob.core.windows.net/dataset>'

[SAS Token](#): ?sv=2019-10-

10&si=prod&sr=c&sig=9qSQZo4ggrCNpybBExU8SypuUZV33igI11xw0P7rB3c%3D

Use Terms

External data users may freely download, analyze, and publish results based on any ENCODE data without restrictions, regardless of type or size, and includes no grace period for ENCODE data producers, either as individual members or as part of the Consortium. Researchers using unpublished ENCODE data are encouraged to contact the data producers to discuss possible publications. The Consortium will continue to publish the results of its own analysis efforts in independent publications.

ENCODE request that researchers who use ENCODE datasets (published or unpublished) in publications and presentations cite the ENCODE Consortium in all of the following ways reported on <https://www.encodeproject.org/help/citing-encode/>.

Contact

If you have any questions, concerns, or comments, email our help desk at encode-help@lists.stanford.edu.

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

GATK Resource Bundle

Article • 04/19/2022

The [GATK resource bundle](#) is a collection of standard files for working with human resequencing data with the GATK.

Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Data source

This dataset is a mirror of the data store at

<https://gatk.broadinstitute.org/hc/articles/360035890811-Resource-bundle>

Data volumes and update frequency

1. datasetgatkbestpractices : 542 GB
2. datasetgatklegacybundles : 61 GB
3. datasetgatktestdata : 2 TB
4. datasetpublicbroadref : 477 GB
5. datasetbroadpublic : 3 TB

Datasets are updated monthly during the first week of every month.

Storage location

This dataset is stored in the West US 2 and West Central US Azure regions. Allocating compute resources in West US 2 or West Central US is recommended for affinity.

Data Access

1. datasetgatkbestpractices

West US 2: 'https://datasetgatkbestpractices.blob.core.windows.net/dataset'

West Central US: 'https://datasetgatkbestpractices-secondary.blob.core.windows.net/dataset'

SAS Token: ?sv=2020-04-

08&si=prod&sr=c&sig=6SaDfKtXAlfdpO%2BkvNA%2FsTNmNij%2Byh%2F%2F%2B
f98WAUqs7I%3D

2. datasetgatklegacybundles

West US 2: 'https://datasetgatklegacybundles.blob.core.windows.net/dataset'

West Central US: 'https://datasetgatklegacybundles-secondary.blob.core.windows.net/dataset'

SAS Token: ?sv=2020-04-

08&si=prod&sr=c&sig=xBfxOPBqHKUCszzwbNCBYF0k9osTQjKnZbEjXCW7gU0%3
D

3. datasetgatktestdata

West US 2: 'https://datasetgatktestdata.blob.core.windows.net/dataset'

West Central US: 'https://datasetgatktestdata-secondary.blob.core.windows.net/dataset'

SAS Token: ?sv=2020-04-

08&si=prod&sr=c&sig=fzLts1Q2vKjuvR7g50vE4HteEHBxTcJbNvf%2FZCeDMO4%3
D

4. datasetpublicbroadref

West US 2: 'https://datasetpublicbroadref.blob.core.windows.net/dataset'

West Central US: 'https://datasetpublicbroadref-secondary.blob.core.windows.net/dataset'

SAS Token: ?sv=2020-04-

08&si=prod&sr=c&sig=DQxmjB4D1lAfOW9AxIWbXwZx6ksbwjLNkixw597JnvQ%3D

5. datasetbroadpublic

West US 2: 'https://datasetbroadpublic.blob.core.windows.net/dataset'

West Central US: 'https://datasetbroadpublic-secondary.blob.core.windows.net/dataset'

SAS Token: ?sv=2020-04-

08&si=prod&sr=c&sig=u%2Bg2Ab7WKZEGiAkwlj6nKiEeZ5wdoJb10Az7uUw is%2Fg%3D

Use Terms

Visit the [GATK resource bundle official site](#).

Contact

Visit the [GATK resource bundle official site](#).

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

Genome Aggregation Database (gnomAD)

Article • 04/19/2022

The [Genome Aggregation Database \(gnomAD\)](#) is a resource developed by an international coalition of investigators, with the goal of aggregating and harmonizing both exome and genome sequencing data from a wide variety of large-scale sequencing projects, and making summary data available for the wider scientific community.

ⓘ Note

Microsoft provides Azure Open Datasets on an “as is” basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Data source

This dataset is hosted as a collaboration with the Broad Institute and the full gnomAD data catalog can be seen at <https://gnomad.broadinstitute.org/downloads>

Data volumes and update frequency

This dataset contains approximately 30 TB of data and is updated with each gnomAD release.

Storage location

The Storage Account hosting this dataset is in the East US Azure region. Allocating compute resources in East US is recommended for affinity.

Data Access

Storage Account: 'https://datasetgnomad.blob.core.windows.net/dataset/'

The data is available publicly without restrictions, and the AzCopy tool is recommended for bulk operations. For example, to view the VCFs in release 3.0 of gnomAD:

PowerShell

```
$ azcopy ls  
https://datasetgnomad.blob.core.windows.net/dataset/release/3.0/vcf/genomes
```

To download all the VCFs recursively:

PowerShell

```
$ azcopy cp --recursive=true  
https://datasetgnomad.blob.core.windows.net/dataset/release/3.0/vcf/genomes  
.
```

NEW: Parquet format of gnomAD v2.1.1 VCF files (exomes and genomes)

To view the parquet files:

PowerShell

```
$ azcopy ls https://datasetgnomadparquet.blob.core.windows.net/dataset
```

To download all the parquet files recursively:

PowerShell

```
$ cp --recursive=true  
https://datasetgnomadparquet.blob.core.windows.net/dataset
```

The [Azure Storage Explorer](#) is also a useful tool for browsing the list of files in the gnomAD release.

Use Terms

Data is available without restrictions. For more information and citation details, see the [gnomAD about page](#).

Contact

For any questions or feedback about this dataset, contact the [gnomAD team](#).

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

Human Reference Genomes

Article • 04/19/2022

This dataset includes two human-genome references assembled by the [Genome Reference Consortium](#): Hg19 and Hg38.

For more information on Hg19 (GRCh37) data, see the [GRCh37 report at NCBI](#).

For more information on Hg38 data, see the [GRCh38 report at NCBI](#).

Other details about the data can be found at [NCBI RefSeq](#) site.

Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Data source

This dataset is sourced from two FTP locations:

ftp://ftp.ncbi.nih.gov/genomes/refseq/vertebrate_mammalian/Homo_sapiens/all_assembly_versions/GCF_000001405.25_GRCh37.p13/

ftp://ftp.ncbi.nih.gov/genomes/refseq/vertebrate_mammalian/Homo_sapiens/latest_assembly_versions/GCF_000001405.39_GRCh38.p13/

Blob names are prefixed beginning with the "vertebrate_mammalian" segment of the URI.

Data volumes and update frequency

This dataset contains approximately 10 GB of data and is updated daily.

Storage location

This dataset is stored in the West US 2 and West Central US Azure regions. Allocating compute resources in West US 2 or West Central US is recommended for affinity.

Data Access

West US 2: 'https://datasetreferencegenomes.blob.core.windows.net/dataset'

West Central US: 'https://datasetreferencegenomes-secondary.blob.core.windows.net/dataset'

SAS Token: sv=2019-02-02&se=2050-01-01T08%3A00%3A00Z&si=prod&sr=c&sig=JtQoPFqjC24GiEB7v9zHLi4RrA2Kd1r%2F3iFt2I9%2FIV8%3D

Use Terms

Data is available without restrictions. For more information and citation details, see the [NCBI Reference Sequence Database site](#).

Contact

For any questions or feedback about this dataset, contact the [Genome Reference Consortium](#).

Data access

Azure Notebooks

azure-storage

💡 Tip

[Download the notebook instead](#).

Getting the Reference Genomes from Azure Open Datasets

Several public genomics data has been uploaded as an Azure Open Dataset [here](#). We create a blob service linked to this open dataset. You can find examples of data calling procedure from Azure Open Datasets for `Reference Genomes` dataset in below:

Users can call and download the following path with this notebook:

```
'https://datasetreferencegenomes.blob.core.windows.net/dataset/vertebrate_mammalian/Homo_sapiens/latest_assembly_versions/GCF_000001405.39_GRCh38.p13/GCF_000001405.39_GRCh38.p13_assembly_structure/genomic_regions_definitions.txt'
```

Important note: Users need to log in their Azure Account via Azure CLI for viewing the data with Azure ML SDK. On the other hand, they do not need do any actions for downloading the data.

[Install the Azure CLI.](#)

Calling the data from 'Reference Genome Datasets'

Python

```
import azureml.core
print("Azure ML SDK Version: ", azureml.core.VERSION)
```

Python

```
from azureml.core import Dataset
reference_dataset =
Dataset.File.from_files('https://datasetreferencegenomes.blob.core.windows.net/dataset')
mount = reference_dataset.mount()
```

Python

```
import os

REF_DIR =
'/vertebrate_mammalian/Homo_sapiens/latest_assembly_versions/GCF_000001405.39_GRCh38.p13/GCF_000001405.39_GRCh38.p13_assembly_structure'
path = mount.mount_point + REF_DIR

with mount:
    print(os.listdir(path))
```

Python

```
import pandas as pd

# create mount context
mount.start()

# specify path to genomic_regions_definitions.txt file
REF_DIR =
'vertetebrate_mammalian/Homo_sapiens/latest_assembly_versions/GCF_00000140
5.39_GRCh38.p13/GCF_000001405.39_GRCh38.p13_assembly_structure'
metadata_filename = '{}{}{}'.format(mount.mount_point, REF_DIR,
'genomic_regions_definitions.txt')

# read genomic_regions_definitions.txt file
metadata = pd.read_table(metadata_filename)
metadata
```

Download the specific file

Python

```
import os
import uuid
import sys
from azure.storage.blob import BlockBlobService, PublicAccess

blob_service_client =
BlockBlobService(account_name='datasetreferencegenomes', sas_token='sv=20
19-02-02&se=2050-01-
01T08%3A00%3A00Z&si=prod&sr=c&sig=JtQoPFqiC24GiEB7v9zHLi4RrA2Kd1r%2F3iFt
219%2F1V8%3D')
blob_service_client.get_blob_to_path('dataset/vertebrate_mammalian/Homo_
sapiens/latest_assembly_versions/GCF_000001405.39_GRCh38.p13/GCF_0000014
05.39_GRCh38.p13_assembly_structure', 'genomic_regions_definitions.txt',
'./genomic_regions_definitions.txt')
```

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

Illumina Platinum Genomes

Article • 04/19/2022

Whole-genome sequencing is enabling researchers worldwide to characterize the human genome more fully and accurately. This requires a comprehensive, genome-wide catalog of high-confidence variants called in a set of genomes as a benchmark. Illumina has generated deep, whole-genome sequence data of 17 individuals in a three-generation pedigree. Illumina has called variants in each genome using a range of currently available algorithms.

For more information on the data, see the official [Illumina site](#).

ⓘ Note

Microsoft provides Azure Open Datasets on an “as is” basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Data source

This dataset is a mirror of <ftp://ussd-ftp.illumina.com/>

Data volumes and update frequency

This dataset contains approximately 2 GB of data and is updated daily.

Storage location

This dataset is stored in the West US 2 and West Central US Azure regions. We recommend locating compute resources in West US 2 or West Central US for affinity.

Data Access

West US 2: 'https://datasetplatinumgenomes.blob.core.windows.net/dataset'

West Central US: 'https://datasetplatinumgenomes-secondary.blob.core.windows.net/dataset'

SAS Token: sv=2019-02-02&se=2050-01-01T08%3A00%3A00Z&si=prod&sr=c&sig=FFfZ0QaDcnEPQmWsshtpoYOjbzd4jtwIWeK%2Fc4i9MqM%3D

Use Terms

Data is available without restrictions. For more information and citation details, see the [official Illumina site](#).

Contact

For any questions or feedback about the dataset, contact platinumgenomes@illumina.com.

Data access

Azure Notebooks

azure-storage



Tip
Download the dataset instead.

Getting the Illumina Platinum Genomes from Azure Open Datasets and Doing Initial Analysis

Use Jupyter notebooks, GATK, and Picard to do the following:

1. Annotate genotypes using VariantFiltration
2. Select Specific Variants
3. Filter the relevant variants- no calls OR specific regions

4. Perform concordance analysis
5. Convert the final VCF files to a table

Dependencies:

This notebook requires the following libraries:

- Azure storage `pip install azure-storage-blob`
- numpy `pip install numpy`
- Genome Analysis Toolkit (GATK) (*Users need to download GATK from Broad Institute's webpage into the same compute environment with this notebook: <https://github.com/broadinstitute/gatk/releases>*)

Important information: This notebook is using Python 3.6 kernel

Getting the Genomics data from Azure Open Datasets

Several public genomics data has been uploaded as an Azure Open Dataset [here](#). We create a blob service linked to this open dataset. You can find examples of data calling procedure from Azure Open Dataset for `Illumina Platinum Genomes` datasets in below:

Downloading the specific 'Illumina Platinum Genomes'

Python

```
import os
import uuid
import sys
from azure.storage.blob import BlockBlobService, PublicAccess

blob_service_client =
BlockBlobService(account_name='datasetplatinumgenomes',
sas_token='sv=2019-02-02&se=2050-01-
01T08%3A00%3A00Z&si=prod&sr=c&sig=FFFZ0QaDcnEPQmWsshtpoY0jbzd4jtwIWeK%2F
c4i9MqM%3D')
blob_service_client.get_blob_to_path('dataset/2017-
1.0/hg38/small_variants/NA12877', 'NA12877.vcf.gz', './NA12877.vcf.gz')
```

1. Annotate genotypes using VariantFiltration

Important note: Check your GATK is running on your system.

If we want to filter heterozygous genotypes, we use VariantFiltration's `--genotype-filter-expression isHet == 1` option. We can specify the annotation value for the tool to label the heterozygous genotypes with the `--genotype-filter-name` option. Here, this parameter's value is set to `isHetFilter`. In our first example, we used `NA12877.vcf.gz` from Illumina Platinum Genomes but users can use any vcf files from other datasets: [Platinum Genomes](#)

Python

```
run gatk VariantFiltration -V NA12877.vcf.gz -O outputannot.vcf --genotype-filter-expression "isHet == 1" --genotype-filter-name "isHetFilter"
```

2. Select Specific Variants

Select a subset of variants from a VCF file. This tool makes it possible to select a subset of variants based on various criteria in order to facilitate certain analyses. Examples of such analyses include comparing and contrasting cases vs. controls, extracting variant or non-variant loci that meet certain requirements, or troubleshooting some unexpected results, to name a few.

There are many different options for selecting subsets of variants from a larger call set:

Extract one or more samples from a call set based on either a complete sample name or a pattern match. Specify criteria for inclusion that place thresholds on annotation values, **for example "DP > 1000"** (depth of coverage greater than 1000x), **"AF < 0.25"** (sites with allele frequency less than 0.25). These criteria are written as "JEXL expressions", which are documented in the article about using JEXL expressions. Provide concordance or discordance tracks in order to include or exclude variants that are also present in other given call sets. Select variants based on criteria like their type (for example, INDELs only), evidence of mendelian violation, filtering status, allelicity, etc. There are also several options for recording the original values of certain annotations, which are recalculated when one subsets the new call set, trims alleles, etc.

Input: A variant call set in VCF format from which a subset can be selected.

Output: A new VCF file containing the selected subset of variants.

Python

```
run gatk SelectVariants -R Homo_sapiens_assembly38.fasta -V
outputannot.vcf --select-type-to-include SNP --select-type-to-include
INDEL -O selective.vcf
```

3. Transform filtered genotypes to no call

Running SelectVariants with --set-filtered-gt-to-nocall will further transform the flagged genotypes with a null genotype call.

This conversion is necessary because downstream tools do not parse the FORMAT-level filter field.

How can we filter the variants with 'No call'

Python

```
run gatk SelectVariants -V outputannot.vcf --set-filtered-gt-to-nocall -
O outputnocall.vcf
```

4. Check the Concordance of VCF file with Ground Truth

Evaluate site-level concordance of an input VCF against a truth VCF. This tool evaluates two variant call sets against each other and produces a six-column summary metrics table.

This function will:

1. Stratifies SNP and INDEL calls
2. Report true-positive, False-positive, and false-negative calls
3. Calculates sensitivity and precision

The tool assumes all records in the --truth VCF are passing truth variants. For the -eval VCF, the tool uses only unfiltered passing calls.

Optionally, the tool can be set to produce VCFs of the following variant records, annotated with each variant's concordance status:

True positives and false negatives (that is, all variants in the truth VCF): useful for calculating sensitivity

True positives and false positives (that is, all variants in the eval VCF): useful for obtaining a training data set for machine learning classifiers of artifacts

These output VCFs can be passed to `VariantsToTable` to produce a TSV file for statistical analysis in R or Python.

Python

```
run gatk Concordance -R Homo_sapiens_assembly38.fasta -eval
outputannot.vcf --truth outputnocall.vcf --summary summary.tsv
```

5. VariantsToTable

Extract fields from a VCF file to a tab-delimited table. This tool extracts specified fields for each variant in a VCF file to a tab-delimited table, which may be easier to work with than a VCF. By default, the tool only extracts PASS or (unfiltered) variants in the VCF file. Filtered variants may be included in the output by adding the `--show-filtered` flag. The tool can extract both INFO (that is, site-level) fields and FORMAT (that is, sample-level) fields.

INFO/site-level fields:

Use the `-F` argument to extract INFO fields; each field will occupy a single column in the output file. The field can be any standard VCF column (for example, CHROM, ID, QUAL) or any annotation name in the INFO field (for example, AC, AF). The tool also supports the following fields:

EVENTLENGTH (length of the event) TRANSITION (1 for a bi-allelic transition (SNP), 0 for bi-allelic transversion (SNP), -1 for INDELs and multi-allelics) HET (count of het genotypes) HOM-REF (count of homozygous reference genotypes) HOM-VAR (count of homozygous variant genotypes) NO-CALL (count of no-call genotypes) TYPE (type of variant, possible values are NO_VARIATION, SNP, MNP, INDEL, SYMBOLIC, and MIXED VAR (count of non-reference genotypes) NSAMPLES (number of samples) NCALLED (number of called samples) MULTI-ALLELIC (is this variant multi-allelic? true/false)

FORMAT/sample-level fields:

Use the `-GF` argument to extract FORMAT/sample-level fields. The tool will create a new column per sample with the name "SAMPLE_NAME.FORMAT_FIELD_NAME" for example, NA12877.GQ, NA12878.GQ.

Input:

A VCF file to convert to a table

Output:

A tab-delimited file containing the values of the requested fields in the VCF file.

Python

```
run gatk VariantsToTable -V NA12877.vcf.gz -F CHROM -F POS -F TYPE -F AC  
-F AD -F AF -GF DP -GF AD -O outputtable.table
```

References

1. VariantFiltration: <https://gatk.broadinstitute.org/hc/en-us/articles/360036827111-VariantFiltration> ↗
2. Select Variants: <https://gatk.broadinstitute.org/hc/en-us/articles/360037052272-SelectVariants>
3. Concordance: <https://gatk.broadinstitute.org/hc/en-us/articles/360041851651-Concordance> ↗
4. Variants to table: <https://gatk.broadinstitute.org/hc/en-us/articles/360036882811-VariantsToTable> ↗
5. Illumina Platinum Genomes: <https://www.illumina.com/platinumgenomes.html>

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

OpenCravat: Open Custom Ranked Analysis of Variants Toolkit

Article • 04/19/2022

OpenCRAVAT is a Python package that performs genomic variant interpretation including variant impact, annotation, and scoring. OpenCRAVAT has a modular architecture with a wide variety of analysis modules and annotation resources that can be selected and installed/run based on the needs of a given study.

For more information on the data, see the [OpenCravat](#).

ⓘ Note

Microsoft provides Azure Open Datasets on an “as is” basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Data source

This dataset is a mirror of the store at <https://store.opencravat.org> and <https://run.opencravat.org>

Data volumes and update frequency

This dataset includes 500 GB of data, and is updated daily.

Storage location

This dataset is stored in the West US 2 and West Central US Azure regions. Allocating compute resources in West US 2 or West Central US is recommended for affinity.

Data Access

West US 2: 'https://datasetopencravat.blob.core.windows.net/dataset'

West Central US: 'https://datasetopencravat-secondary.blob.core.windows.net/dataset'

SAS Token: sv=2020-04-08&st=2021-03-11T23%3A50%3A01Z&se=2025-07-26T22%3A50%3A00Z&sr=c&sp=rl&sig=J9J9wnJOXsmEy7TFMq9wjcjXDE%2B7KhGpCU L4elsC14%3D

Use Terms

OpenCRAVAT is available with a GPLv3 license. Most data sources are free for non-commercial use. For commercial use, consult the institutional contacts for each data source.

Contact

rkarchi1@jhmi.edu

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

SnpEff: Genomic variant annotations and functional effect prediction toolbox

Article • 04/19/2022

[SnpEff](#) Genetic variant annotation and functional effect prediction toolbox. It annotates and predicts the effects of genetic variants on genes and proteins (such as amino acid changes).

For more information on the data, see the [User Manual](#).

Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Data source

This dataset is a mirror of <http://downloads.sourceforge.net/project/snpeff/databases/>

Data volumes and update frequency

This dataset contains approximately 2 TB of data and is updated monthly.

Storage location

This dataset is stored in the West US 2 and West Central US Azure regions. Allocating compute resources in West US 2 or West Central US is recommended for affinity.

Data Access

West US 2: '<https://datasetsnpeff.blob.core.windows.net/dataset>'

West Central US: 'https://datasetsnpeff-secondary.blob.core.windows.net/dataset'

SAS Token: sv=2019-10-10&st=2020-09-01T00%3A00%3A00Z&se=2050-09-01T00%3A00%3A00Z&si=prod&sr=c&sig=isafOa9tGnYBAvsXFUMGMTbsG2z%2FShaihzp7JE5dHw%3D

Use Terms

Data is available without restrictions. More information and citation details, see [Accessing and using data in ClinVar](#).

Contact

For any questions or feedback about this dataset, contact [Pablo Cingolani](#).

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

Electronic Prescriptions for Controlled Substances (EPCS)

Article • 12/05/2022

EPCS overview

The US Drug Enforcement Administration (DEA) [Electronic Prescriptions for Controlled Substances](#) (EPCS) is a rule that went into effect on 1 June 2010. It revised DEA regulations for prescribers and pharmacies, allowing the e-prescribing of controlled substances. The regulation provides pharmacies, hospitals, and practitioners with the ability to use modern technology for controlled substance prescriptions while maintaining the closed system of controls on controlled substances. Prescribers can digitally sign, transmit, report, and archive electronic prescriptions, while pharmacies can receive, dispense, and archive these electronic prescriptions.

The regulation covers:

- Logical access controls for both prescribers and pharmacy systems
- Multi-factor authentication for prescribers and administrators of prescribers
- Digital signing of prescriptions for prescribers
- Record keeping for both prescribers and pharmacies
- Reporting and auditing of both prescribers and pharmacies
- Data backups and archiving for both prescribers and pharmacies

DEA uses the following definitions for multi-factor authentication (MFA):

- Two-factor credentials
 - Something you know – a knowledge factor
 - Something you have – a hard token stored separately from the computer being accessed
 - Something you are – biometric information
- Hard token
 - A cryptographic key stored on or a one-time password (OTP) transmitted to a specialized hardware device (for example, a PDA, mobile phone, smart card, USB key) rather than a general-purpose computer.

For more information, see [Title 21 Code of Federal Regulations Part 1311.115](#) *Additional requirements for two-factor authentication.*

EPCS multi-factor authentication requirements

In EPCS, the DEA provides several requirements related to MFA for administrators of prescribing systems, prescribers, and digital signing.

- Two-factor authentication must be used to assign a prescriber within the electronic system, approve a prescription entry, and digitally sign a prescription.
- Two of the factors must be of the following three options: a username/password, a hard token, or a biometric identification. The DEA has stated that the use of a type of token or OTP generator must meet the same requirements as defined for a hard token under the current regulation.
- If a hard token is used, it must meet FIPS 140 Security Level 1 for cryptographic devices or OTP devices.
- The hard token must be stored on a device that is separate from the computer being used to access the application.

EPCS token requirements and FIPS 140

The [Federal Information Processing Standard \(FIPS\) 140](#) is a US government standard that defines minimum security requirements for cryptographic modules in information technology products and systems. Testing against the FIPS 140 standard is maintained by the [Cryptographic Module Validation Program](#) (CMVP), a joint effort between the US National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security, a branch of the Communications Security Establishment (CSE) of Canada. For more information, see [Azure FIPS 140 documentation](#).

EPCS requires that solutions for **hard tokens** use cryptographic modules validated at FIPS 140 Level 1 to ensure end users receive a high degree of security, assurance, and non-repudiation. For more information, see [Title 21 Code of Federal Regulations Part 1311.115](#) *Additional requirements for two-factor authentication*. The types of hard tokens commonly used have either a cryptographic module as part of the token itself or a random number generator, also called an OTP generator.

Azure and EPCS multi-factor authentication

As mentioned previously, two of the factors for EPCS multi-factor authentication must be of the following three options:

1. Username/password
2. Hard token
3. Biometric identification

This section focuses on Azure support for **hard tokens** to meet EPCS multi-factor requirements. There are several requirements specific to biometrics, as described in [Title](#)

21 Code of Federal Regulations Part 1311.116 [Additional requirements for biometrics.](#)

However, these requirements aren't applicable to Azure.

The [Microsoft Authenticator app](#) provides an extra level of security to your Azure AD account. It's available on mobile phones running Android and iOS. With the Microsoft Authenticator app, you can provide secondary verification for MFA scenarios to meet your EPCS MFA requirements. As mentioned previously, EPCS requires that solutions for hard tokens use cryptographic modules validated at FIPS 140 Level 1 to ensure end users receive a high degree of security, assurance, and non-repudiation. The Microsoft Authenticator app meets FIPS 140 Level 1 validation requirements for all Azure AD authentications, as explained in [Authentication methods in Azure Active Directory - Microsoft Authenticator app](#). FIPS 140 compliance for Microsoft Authenticator is currently in place for iOS and in progress for Android.

Moreover, Azure can help you meet and **exceed** your EPCS MFA requirements by supporting the highest Authenticator Assurance Level 3 (AAL3), as described in the National Institute of Standards and Technology (NIST) [SP 800-63](#) *Digital Identity Guidelines*. According to [NIST SP 800-63B Section 4.3](#), multi-factor **authenticators** used at AAL3 shall rely on hardware cryptographic modules validated at FIPS 140 Level 2 overall with at least FIPS 140 Level 3 for physical security, which exceeds the EPCS MFA requirements. **Verifiers** at AAL3 shall be validated at FIPS 140 Level 1 or higher.

Azure Active Directory (Azure AD) supports both authenticator and verifier NIST SP 800-63B AAL3 requirements:

- **Authenticator requirements:** FIDO2 security keys, smartcards, and Windows Hello for Business can help you meet AAL3 requirements, including the underlying FIPS 140 validation requirements. Azure AD support for NIST SP 800-63B AAL3 **exceeds** the EPCS multi-factor authentication requirements.
- **Verifier requirements:** Azure AD uses the [Windows FIPS 140 Level 1](#) overall validated cryptographic module for all its authentication related cryptographic operations. It is therefore a FIPS 140 compliant verifier.

For more information, see [Azure NIST SP 800-63 documentation](#).

Applicability

- Azure
- Azure Government

Guidance documents

Microsoft provides detailed guidance that is relevant to EPCS multi-factor authentication:

- How to configure Azure AD to meet NIST SP 800-63B Authenticator Assurance Levels, including AAL1, AAL2, and AAL3. For more information, see [Achieving NIST AALs](#).
- How to configure controls in the Access Control (AC) and Identification and Authentication (IA) control families to meet FedRAMP High requirements. For more information, see [Configure Azure AD to meet FedRAMP High](#).

Frequently asked questions

Can Azure support my EPCS multi-factor authentication requirements?

Yes. Azure can help you meet your EPCS multi-factor authentication requirements because Azure AD supports both authenticator and verifier [NIST SP 800-63B](#)  Authenticator Assurance Level 3 (AAL3) requirements, including FIPS 140 validation at the requisite level. Azure AD exceeds the EPCS multi-factor authentication requirements. We recommend using a multi-factor cryptographic hardware authenticator to achieve AAL3. FIDO2 security keys, smartcards, and Windows Hello for Business can help you meet AAL3 requirements, which in turn cover EPCS multi-factor authentication requirements. For more information, see [Azure NIST SP 800-63 documentation](#). You can also use the [Microsoft Authenticator app](#), which meets FIPS 140 Level 1 validation requirements for all Azure AD authentications, as explained in [Authentication methods in Azure Active Directory - Microsoft Authenticator app](#).

Does Microsoft provide guidance on achieving NIST SP 800-63B AAL3 requirements?

Yes. For more information, see [Guidance documents](#).

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](#) 
- [Electronic Prescriptions for Controlled Substances](#)  (EPCS)
- [NIST SP 800-63](#)  *Digital Identity Guidelines*
- [NIST SP 800-63A](#)  *Enrollment and Identity Proofing*
- [NIST SP 800-63B](#)  *Authentication and Lifecycle Management*

- NIST SP 800-63C  *Federation and Assertions*

GxP (FDA 21 CFR Part 11)

Article • 01/31/2023

GxP (FDA 21 CFR Part 11) overview

The term *GxP* is a general abbreviation for *good practice* guidelines and regulations in the life sciences industry, including good clinical, laboratory, manufacturing, and other practices. There is no single regulatory entity or administration; each country has its own guidelines and regulators, although requirements are similar from country to country.

For example, GxP requirements are outlined in the following regulations:

- [Title 21 CFR Part 11](#) as enforced by the Food and Drug Administration (FDA) in the United States.
- [EudraLex Volume 4 – GMP Guidelines, Annex 11](#) in the European Union.

Regulatory goals help ensure that businesses in regulated industries manufacture products that are safe to use and meet stringent quality standards during the production process. Computerized systems that use GxP processes require validation of adherence to GxP requirements, and are considered qualified when the system can demonstrate ability to fulfill them.

Azure and GxP (FDA 21 CFR Part 11)

Azure can help you meet your GxP requirements and regulations enforced by the FDA under 21 CFR Part 11. There is no GxP or FDA 21 CFR Part 11 certification for cloud service providers; however, Azure has undergone independent third-party audits for quality management and information security, including [ISO 9001](#) and [ISO/IEC 27001](#) among many others. If you are deploying applications on Azure, you should determine the GxP requirements that apply to the computerized system based on its intended use. You should then follow internal procedures governing qualification and/or validation processes to demonstrate that the GxP requirements are met.

You should review the white paper [Strategies for life sciences companies using Microsoft Azure with GxP systems](#) produced by Accenture to:

- Learn how to analyze controls required to use Azure,
- Define how Azure can meet those controls, and
- Define the levels of ownership from a life sciences company's perspective when validating and maintaining GxP systems hosted on Azure.

Among other things, the white paper shows how certain FDA regulations, such as 21 CFR Part 820 and 21 CFR Part 11, apply to Azure.

Moreover, Microsoft retained Montrium, an independent organization specializing in quality assurance and regulatory GxP compliance for the life sciences industry, to conduct the Azure GxP qualification review. If you're a regulated customer within the life sciences industry, aiming to use the Azure platform to host GxP regulated computerized systems, you should review the resulting [Microsoft Azure GxP guidelines](#). The guidelines document identifies the responsibilities shared by Microsoft and you for meeting:

- FDA 21 CFR Part 11 regulatory requirements for electronic records and signatures
- EudraLex Volume 4 – Annex 11 for computerized systems

It describes recommended activities and controls that you can establish to qualify and maintain control over the GxP computerized systems deployed on the Azure platform. The qualification approach outlined in this document is based on industry best practices with an emphasis on the concepts presented and described within:

- The International Society for Pharmaceutical Engineering (ISPE) Good Automated Manufacturing Practices (GAMP) series of [Good Practice Guides](#)
- The Pharmaceutical Inspection Co-operation Scheme (PIC/S) [PI 011-3 Good Practices for Computerised Systems in Regulated GxP Environments](#)

Dynamics 365 and Power Platform support for GxP (FDA 21 CFR Part 11)

While considering the use of cloud services to host GxP content, it's important for life sciences organizations to assess the adequacy of the cloud service provider's processes and controls that help ensure the confidentiality, integrity, and availability of data that's stored in the cloud. When stored in Microsoft Dynamics 365 and Power Platform, your customer data benefits from multiple layers of security and governance technologies, operational practices, and compliance policies to enforce data privacy and integrity at specific levels. To help demonstrate how you can develop and operate GxP applications on Microsoft Dynamics 365 and Power Platform with confidence and remain compliant while using Microsoft cloud services, Microsoft published the following document:

- [Microsoft GxP guidelines for Dynamics 365 and Power Platform](#)

This guidance document highlights the extensive controls implemented as part of Dynamics 365 and Power Platform's internal development of security and quality practices. These practices help ensure that Dynamics 365 and Power Platform meet their

specifications and are maintained in a state of control. Dynamics 365 and Power Platform procedural and technical controls are regularly audited and verified for effectiveness by independent third-party assessors.

Applicability

- Azure
- Azure Government

Office 365 and GxP (FDA 21 CFR Part 11)

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

Guidance documents

- [Strategies for life sciences companies using Microsoft Azure with GxP systems](#) ↗ produced by Accenture
- [Microsoft Azure GxP guidelines](#) ↗ produced by Montrium
- [Microsoft GxP guidelines for Dynamics 365 and Power Platform](#) ↗

Frequently asked questions

Can I use Microsoft GxP guidelines in my organization's GxP compliance efforts?

If you're deploying applications on Azure or storing data in Dynamics 365 and Power Platform, you should determine the GxP requirements that apply to your computerized systems based on the intended use and then follow internal procedures governing qualification and validation processes to demonstrate that you have met those requirements.

Can I use Microsoft's compliance assurances in the certification process for my organization?

Yes. The independent third-party audit reports and certificates for standards such as the ISO 27001, ISO 27018, ISO 9001, SOC 1, and SOC 2 attest to the effectiveness of Microsoft controls. You may use the audited controls described in these reports as part of your own GxP or FDA 21 CFR Part 11 qualification efforts. If you build and deploy applications subject to FDA regulation, you're responsible for ensuring that your applications meet FDA requirements.

Resources

- Azure compliance documentation
- Azure enables a world of compliance ↗
- Microsoft 365 compliance offerings
- Compliance on the Microsoft Trust Center ↗
- Azure for healthcare ↗
- Azure high-performance computing for health and life sciences ↗
- Microsoft Cloud for healthcare ↗
- Microsoft Cloud for life sciences ↗

HIPAA (US)

Article • 04/06/2023

HIPAA overview

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the regulations issued under HIPAA are a set of US healthcare laws that, among other provisions, establish requirements for the use, disclosure, and safeguarding of protected health information (PHI). The scope of HIPAA was extended in 2009 with the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act that was created to stimulate the adoption of electronic health records and supporting information technology.

HIPAA applies to covered entities – doctors' offices, hospitals, health insurers, and other healthcare companies – that create, receive, maintain, transmit, or access PHI. HIPAA further applies to business associates of covered entities that perform certain functions or activities involving PHI as part of providing services to the covered entity or on behalf of the covered entity. When a covered entity engages the services of a cloud service provider (CSP), such as Microsoft, the CSP becomes a business associate under HIPAA. Moreover, when a business associate subcontracts with a CSP to create, receive, maintain, or transmit PHI, the CSP also becomes a business associate.

Together, HIPAA and HITECH Act rules include:

- The [Privacy Rule](#), which requires appropriate safeguards to protect the privacy of PHI and imposes restrictions on the use and disclosure of PHI without patient authorization. It also gives patients the rights over their health information, including rights to examine their health records and request corrections.
- The [Security Rule](#), which sets the standards for administrative, technical, and physical safeguards to ensure the confidentiality, integrity, and security of electronic PHI.
- The [Breach Notification Rule](#), which requires covered entities and their business associates to provide notification when a breach of unsecured PHI occurs.

HIPAA regulations require that covered entities and their business associates enter into a contract called a Business Associate Agreement (BAA) to ensure the business associates protect PHI adequately. Among other things, a BAA establishes the permitted and required uses and disclosures of PHI by the business associate, based on the relationship between the parties and the activities and services being performed by the business associate.

Azure and HIPAA

There is currently no certification program approved by the US Department of Health and Human Services (HHS) through which a CSP acting as a business associate could demonstrate compliance with HIPAA and the HITECH Act. However, HIPAA and HITECH Act requirements have been mapped to other established security frameworks and standards that CSPs typically attest to:

- The National Institute of Standards and Technology (NIST) [SP 800-66](#) *An Introductory Resource Guide for Implementing the HIPAA Security Rule*, which addresses security concepts in the HIPAA Security Rule and explains how they relate to other NIST publications on information security. Specifically, Appendix D – Security Rule Standards and Implementation Specifications Crosswalk provides a catalog of the HIPAA Security Rule standards and implementation specifications, and maps each to relevant security controls detailed in [NIST SP 800-53](#) *Security and Privacy Controls for Information Systems and Organizations*. NIST SP 800-53 serves as the baseline control set for the US Federal Risk and Authorization Management Program (FedRAMP). Therefore, a FedRAMP assessment and authorization provides strong assurances that HIPAA Security Rule safeguard standards and specifications are addressed adequately. Both Azure and Azure Government maintain a [FedRAMP High](#) Provisional Authorization to Operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB).
- The Cloud Security Alliance (CSA) [Cloud Controls Matrix](#) (CCM), which maps HIPAA and HITECH Act requirements to CCM control objectives covering fundamental security principles across CCM domains. Both Azure and Azure Government maintain the [CSA STAR Certification](#) and [CSA STAR Attestation](#) that are based on the CCM.
- The HHS [HIPAA Security Rule Crosswalk to NIST Cyber Security Framework](#), which maps each administrative, physical and technical safeguard standard and implementation specification in the HIPAA Security Rule to a relevant NIST Cybersecurity Framework (CSF) subcategory, and provides relevant control mapping to other standards including ISO/IEC 27001 and NIST SP 800-53. Both Azure and Azure Government align with the [NIST CSF](#) and are certified under [ISO/IEC 27001](#).

To support our customers who are subject to HIPAA compliance, Microsoft will enter into BAAs with its covered entity and business associate customers. Azure has enabled the physical, technical, and administrative safeguards required by HIPAA and the HITECH Act inside the in-scope Azure services, and offers a [HIPAA BAA](#) as part of the Microsoft [Product Terms](#) (formerly Online Services Terms) to all customers who are covered entities or business associates under HIPAA for use of such in-scope Azure

services. In the BAA, Microsoft makes contractual assurances about data safeguarding, reporting (including breach notifications), data access in accordance with HIPAA and the HITECH Act, and many other important provisions. Microsoft enables you in your compliance with HIPAA and the HITECH Act, and adheres to the HIPAA Security Rule requirements in its capacity as a business associate.

[Azure Policy regulatory compliance built-in initiative for HIPAA/HITRUST](#) maps to HIPAA/HITRUST **compliance domains** and **controls**. 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 HIPAA/HITRUST 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 Microsoft cloud services in scope for the HIPAA BAA coverage, see [Cloud services in audit scope](#).

Office 365 and HIPAA

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

Guidance documents

- [A practical guide to designing secure health solutions using Microsoft Azure](#)
- [Azure Policy regulatory compliance built-in initiative for HIPAA/HITRUST](#)

Frequently asked questions

How can my organization sign a BAA for Microsoft Azure?

There is no separate contract to sign to enter into a HIPAA Business Associate Agreement (BAA) with Microsoft because the [HIPAA BAA](#) is available via the Microsoft Product Terms (formerly Online Services Terms) by default to all customers who are covered entities or business associates under HIPAA. The Microsoft Product Terms references the Microsoft Products and Services [Data Protection Addendum](#) (DPA), which states that "execution of customer's volume licensing agreement includes execution of the HIPAA Business Associate Agreement".

As explained in the Microsoft Azure Legal Information [Service Agreement & Terms](#), the licensing agreements under which customers purchase Azure incorporate the Microsoft Product Terms and the Microsoft Products and Services Data Protection Addendum (DPA).

I have a healthcare SaaS solution deployed on Azure. Do my customers need to sign a BAA with Microsoft?

No. Microsoft HIPAA BAA is applicable to Microsoft Online Services such as Azure and made available by default to Microsoft customers via a licensing agreement execution that includes the Microsoft Product Terms (formerly Online Services Terms) and the Microsoft Products and Services Data Protection Addendum (DPA). If you're a SaaS provider of a healthcare solution deployed on Azure, your customers who are healthcare providers or covered entities under HIPAA can sign a BAA directly with you. They don't need to have a BAA in place with Microsoft to use your SaaS solution. The Microsoft BAA terms incorporated into your licensing agreement with Microsoft wouldn't be applicable to your customers unless they also happen to be Microsoft customers and have separate licensing agreements in place with Microsoft.

Does having a BAA with Microsoft ensure my organization's compliance with HIPAA?

No. By offering a BAA, Microsoft helps support your HIPAA compliance, but using Azure or other Microsoft cloud services doesn't automatically impart compliance onto your cloud solutions. Your organization is responsible for ensuring that you have an adequate compliance program and internal processes in place, and that your particular use of Azure aligns with HIPAA and the HITECH Act. Microsoft doesn't inspect, approve, or monitor your applications deployed on Azure. You're wholly responsible for ensuring your own compliance with all applicable laws and regulations.

Can Microsoft use my organization's BAA?

No. Microsoft can't use a customer's BAA. Because we offer hyper-scale, multi-tenant cloud services that are standardized for all customers, we must operate our services in a consistent manner. The Microsoft HIPAA BAA reflects closely how we operate our cloud

services. To address the needs of the healthcare industry, Microsoft collaborated with a consortium of academic medical centers and other public and private sector entities within healthcare to create a BAA that aligns with our hyper-scale cloud services and meets customer needs.

Resources

- [Azure compliance documentation](#)
- [Azure enables a world of compliance](#)
- [Microsoft 365 compliance offerings](#)
- [Compliance on the Microsoft Trust Center](#)
- [Microsoft Product Terms](#) (formerly Online Services Terms)
- Microsoft Products and Services [Data Protection Addendum](#) (DPA)
- [Microsoft HIPAA BAA](#)
- HIPAA Privacy Rule [45 CFR Part 160](#) and [45 CFR Part 164](#)
- [HIPAA Omnibus Final Rule](#)
- [Microsoft Cloud for healthcare compliance offerings](#)
- [Azure for healthcare](#)
- [Azure high-performance computing for health and life sciences](#)
- [Microsoft Cloud for healthcare](#)

HITRUST

Article • 04/05/2023

HITRUST overview

[HITRUST](#) is an organization governed by representatives from the healthcare industry. HITRUST created and maintains the [Common Security Framework \(CSF\)](#), a certifiable framework to help healthcare organizations and their providers demonstrate their security and compliance in a consistent and streamlined manner. The CSF builds on [HIPAA and the HITECH Act](#), and incorporates healthcare-specific security, privacy, and other regulatory requirements from existing frameworks such as the [PCI DSS](#), [ISO/IEC 27001](#), and [MARS-E](#).

The CSF contains 14 control categories, comprised of 49 control objectives and 156 control specifications. HITRUST certifies IT offerings against these controls. HITRUST also adapts requirements for certification to the risks of an organization based on organizational, regulatory, and system factors.

HITRUST provides a benchmark—a standardized compliance framework, assessment, and certification process—against which cloud service providers and covered healthcare entities can measure compliance. HITRUST offers three degrees of assurance, or assessment levels:

- Self-assessment performed by an organization, which in turn generates a HITRUST readiness assessment report. This report can't be certified; however, it can be used as a foundation for a validated assessment.
- HITRUST CSF Validated
- HITRUST CSF Validated Certified

Validated assessments are performed onsite by a HITRUST authorized external assessor. Each level builds with increasing rigor on the one below it. An organization with the highest level, CSF Validated Certified, meets all the CSF certification requirements.

Azure and HITRUST

Microsoft Azure is one of the first hyper-scale cloud services platforms to receive a formal certification for the HITRUST CSF in Nov-2016. Azure has maintained the HITRUST CSF certification since then.

For extra customer assistance, Microsoft provides [Azure Policy regulatory compliance built-in initiative for HIPAA/HITRUST](#), which maps to **HIPAA/HITRUST compliance domains** and **controls**. 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 HIPAA/HITRUST 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.

Using the [HITRUST shared responsibility and inheritance program](#), you can accelerate achieving HITRUST compliance for your solutions hosted on Azure. The program enables you to pre-populate your assessment with fully inherited or shared responsibility controls for Azure in the HITRUST MyCSF tool. You can also collaborate with Microsoft on your assessment.

Applicability

- Azure
- Azure Government

Services in scope

For a list of Microsoft cloud services in audit scope, see the Azure HITRUST certification letter or [Cloud services in audit scope](#):

- Azure
- Dynamics 365
- Microsoft 365
- Power Platform

Office 365 and HITRUST

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

Attestation documents

The Azure HITRUST certification letter covers Azure, Dynamics 365, Power Platform, and select Microsoft 365 cloud services. You can access Azure HITRUST audit documents from the Service Trust Portal (STP) [Healthcare and Life Sciences](#) section. For instructions on how to access audit reports and certificates, see [Audit documentation](#).

Moreover, the Azure [HITRUST shared responsibility matrix](#) is available directly from HITRUST. It lists HITRUST CSF controls, [clarifies shared responsibility](#) per control (customer, shared, or Azure), and provides Azure control implementation details where appropriate.

Frequently asked questions

Can I use the Azure HITRUST certification to support my organization's certification process?

Yes. If your business requires HITRUST certification for implementations deployed on Azure, you can build on Azure HITRUST certification when you conduct your compliance assessment. However, you're responsible for evaluating the HITRUST requirements and controls within your own organization.

Does Microsoft certification mean that if my organization uses Azure, it is HITRUST compliant?

No. You're ultimately responsible for your own HITRUST CSF compliance. The Azure HITRUST shared responsibility matrix describes various responsibilities that are owned by Microsoft, you as the customer, or shared by both to achieve HITRUST CSF compliance. In all assessments, proper scoping is key to success. For cloud deployments, you should analyze the HITRUST CSF requirements to understand their intent. Correlating your responsibilities based on the shared responsibility matrix will aid you in planning ahead for a successful assessment.

As a cloud service provider, Microsoft Azure allows you to satisfy specific HITRUST CSF requirements through usage of the HITRUST CSF Inheritance Program. This reliance is dependent on which Azure offerings you're using and how you implemented them.

Most requirements, however, require an understanding of the distribution of responsibilities between you and Azure to fully meet HITRUST CSF compliance. In addition, some requirements are entirely part of your implementation responsibility to meet HITRUST CSF compliance.

How can I get the Azure HITRUST audit documentation?

For links to audit documentation, see [Attestation documents](#).

How do I engage with Microsoft?

Sign in to the HITRUST MyCSF tool and pre-populate your assessment for your solution hosted on Microsoft Azure with either fully inherited or shared responsibility controls for Azure. A Microsoft HITRUST administrator will then complete the Microsoft part of the assessment in the MyCSF tool.

Resources

- [Azure compliance documentation](#)
- [Azure enables a world of compliance](#)
- [Microsoft 365 compliance offerings](#)
- [Compliance on the Microsoft Trust Center](#)
- [HITRUST](#)
- [HITRUST CSF](#)
- [Understanding and leveraging the CSF](#)
- [HITRUST shared responsibility and inheritance program](#)
- [Microsoft Cloud for healthcare compliance offerings](#)
- [Azure for healthcare](#)
- [Azure high-performance computing for health and life sciences](#)
- [Microsoft Cloud for healthcare](#)

HIPAA and HITRUST compliant health data AI

Azure Blob Storage

Azure Event Grid

Azure Functions

Azure Machine Learning

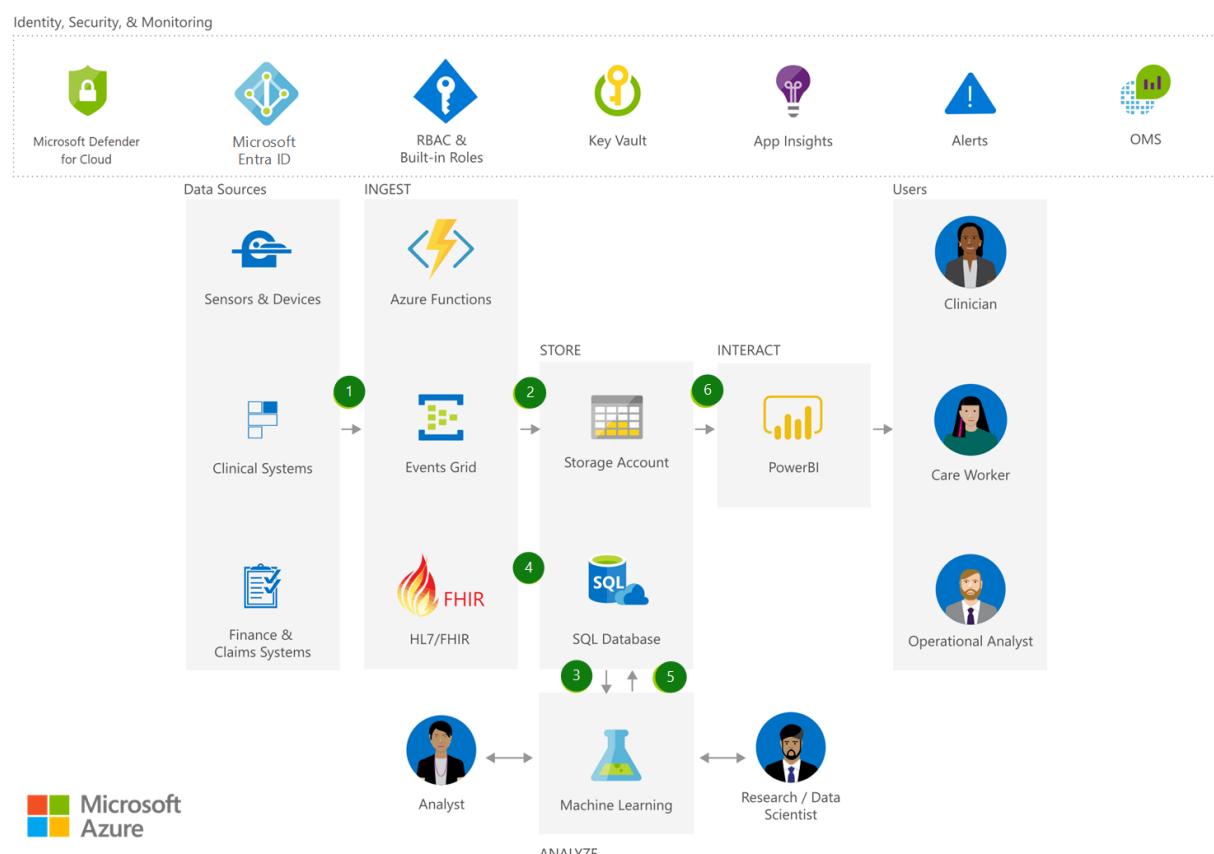
Power BI

💡 Solution ideas

This article is a solution idea. If you'd like us to expand the content with more information, such as potential use cases, alternative services, implementation considerations, or pricing guidance, let us know by providing [GitHub feedback](#).

This article describes how you can store, manage, and analyze HIPAA-compliant and HITRUST-compliant health data and medical records with a high level of built-in security.

Architecture



Download an [SVG](#) of this architecture.

Dataflow

1. Securely ingest bulk patient data into [Azure Blob storage](#).
2. [Event Grid](#) publishes patient data to [Azure Functions](#) for processing, and securely stores patient data in [SQL Database](#).
3. Analyze patient data using [Machine Learning](#), and create a Machine Learning-trained model.
4. Ingest new patient data in HL7/FHIR format and publish to [Azure Functions](#) for processing. Store in [SQL Database](#).
5. Analyze newly ingested data using the trained Machine Learning model.
6. Interact with patient data using [Power BI](#) while preserving Azure role-based access control (Azure RBAC).

Components

- [Azure Functions](#): Process events with serverless code
- [Event Grid](#): Get reliable event delivery at massive scale
- [Storage Accounts](#): Durable, highly available, and massively scalable cloud storage
- [Azure SQL Database](#): Managed, intelligent SQL in the cloud
- [Azure Machine Learning](#): Bring AI to everyone with an end-to-end, scalable, trusted platform with experimentation and model management
- [Power BI Embedded](#): Embed fully interactive, stunning data visualizations in your applications
- [Defender for Cloud](#): Unify security management and enable advanced threat protection across hybrid cloud workloads
- [Microsoft Entra ID](#): Synchronize on-premises directories and enable single sign-on
- [Key Vault](#): Safeguard and maintain control of keys and other secrets
- Application Insights: Detect, triage, and diagnose issues in your web apps and services
- [Azure Monitor](#): Full observability into your applications, infrastructure, and network
- [Operation Management Suite](#): A collection of management services that were designed in the cloud from the start
- [Azure RBAC and built-in roles](#): Azure role-based access control (Azure RBAC) has several built-in role definitions that you can assign to users, groups, and service principals.

Scenario details

This solution demonstrates how you can store, manage, and analyze HIPAA-compliant and HITRUST-compliant health data and medical records with a high level of built-in security.

Potential use cases

This solution is ideal for the medical and healthcare industry.

Next steps

- [Azure Functions Documentation](#)
- [Azure Event Grid Documentation](#)
- [Azure Storage Documentation](#)
- [Azure SQL Database Documentation](#)
- [Azure Machine Learning Documentation](#)
- [Power BI Embedded Documentation](#)
- [Microsoft Defender for Cloud Documentation](#)
- [Get started with Microsoft Entra ID](#)
- [What is Azure Key Vault?](#)
- [What is Application Insights?](#)
- [Monitoring Azure applications and resources](#)
- [What is Operations Management Suite \(OMS\)?](#)
- [Built-in roles for Azure role-based access control](#)

Related resources

- [Health data consortium on Azure](#)
- [Virtual health on Microsoft Cloud for Healthcare](#)
- [Confidential computing on a healthcare platform](#)

Details of the HIPAA HITRUST 9.2 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 HIPAA HITRUST 9.2. For more information about this compliance standard, see [HIPAA HITRUST 9.2](#). To understand *Ownership*, see [Azure Policy policy definition](#) and [Shared responsibility in the cloud](#).

The following mappings are to the **HIPAA HITRUST 9.2** 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 **HITRUST/HIPAA** Regulatory Compliance built-in initiative definition.

This built-in initiative is deployed as part of the [HIPAA HITRUST 9.2 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](#).

Privilege Management

The organization facilitates information sharing by enabling authorized users to determine a business partner's access when discretion is allowed as defined by

the organization and by employing manual processes or automated mechanisms to assist users in making information sharing/collaboration decisions.

ID: 1149.01c2System.9 - 01.c Ownership: Customer

[] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Role-Based Access Control (RBAC) should be used on Kubernetes Services ↗	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	1.0.3 ↗

Contractors are provided with minimal system and physical access only after the organization assesses the contractor's ability to comply with its security requirements and the contractor agrees to comply.

ID: 1154.01c3System.4 - 01.c Ownership: Customer

[] 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 ↗

User Authentication for External Connections

Remote access by vendors and business partners (e.g., for remote maintenance) is disabled/deactivated when not in use.

ID: 1117.01j1Organizational.23 - 01.j Ownership: Customer

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

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

If encryption is not used for dial-up connections, the CIO or his/her designated representative provides specific written authorization.

ID: 1173.01j1Organizational.6 - 01.j Ownership: Customer

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

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

The organization protects wireless access to systems containing sensitive information by authenticating both users and devices.

ID: 1174.01j1Organizational.7 - 01.j Ownership: Customer

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

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 ↗

The organization requires a callback capability with re-authentication to verify dial-up connections from authorized locations.

ID: 1176.01j2Organizational.5 - 01.j Ownership: Customer

[\[+\] 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 ↗

User IDs assigned to vendors are reviewed in accordance with the organization's access review policy, at a minimum annually.

ID: 1177.01j2Organizational.6 - 01.j Ownership: Customer

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

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

User Identification and Authentication

Non-organizational users (all information system users other than organizational users, such as patients, customers, contractors, or foreign nationals), or processes acting on behalf of non-organizational users, determined to need access to information residing on the

organization's information systems, are uniquely identified and authenticated.

ID: 11110.01q1Organizational.6 - 01.q Ownership: Customer

[] [Expand table](#)

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

The organization requires that electronic signatures, unique to one individual, cannot be reused by, or reassigned to, anyone else.

ID: 11208.01q1Organizational.8 - 01.q Ownership: Customer

[] [Expand table](#)

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

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records.

ID: 11210.01q2Organizational.10 - 01.q Ownership: Customer

[] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit Windows machines that have the specified members in the Administrators group 🔗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol 🔗 . Machines are non-compliant if the local Administrators group contains one or more of the members listed in the policy parameter.	auditIfNotExists	2.0.0 🔗

Signed electronic records shall contain information associated with the signing in human-readable format.

ID: 11211.01q2Organizational.11 - 01.q Ownership: Customer

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit Windows machines missing any of specified members in the Administrators group 🔗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol 🔗 . Machines are non-compliant if the local Administrators group does not contain one or more members that are listed in the policy parameter.	auditIfNotExists	2.0.0 🔗

01 Information Protection Program

0101.00a1Organizational.123-00.a 0.01 Information Security Management Program

ID: 0101.00a1Organizational.123-00.a 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	1.1.0 🔗
Establish an information security	CMA_0263 - Establish an information	Manual,	1.1.0 🔗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
program ↗	security program	Disabled	
Protect the information security program plan ↗	CMA_C1732 - Protect the information security program plan	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 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗

0102.00a2Organizational.123-00.a 0.01 Information Security Management Program

ID: 0102.00a2Organizational.123-00.a Ownership: Shared

[\[\]](#) Expand table

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 ↗
Review and update the information security architecture ↗	CMA_C1504 - Review and update the information security architecture	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗

0103.00a3Organizational.1234567-00.a 0.01 Information Security Management Program

ID: 0103.00a3Organizational.1234567-00.a 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	1.1.0 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗

0104.02a1Organizational.12-02.a 02.01 Prior to Employment

ID: 0104.02a1Organizational.12-02.a Ownership: Shared

C 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 ↗
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 personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	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 ↗
Identify individuals with security roles and responsibilities ↗	CMA_C1566 - Identify individuals with security roles and responsibilities	Manual, Disabled	1.1.1 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0 ↗
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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide security training before providing access ↗	CMA_0418 - Provide security training before providing access	Manual, Disabled	1.1.0 ↗
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0 ↗

0105.02a2Organizational.1-02.a 02.01 Prior to Employment

ID: 0105.02a2Organizational.1-02.a Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign risk designations ↗	CMA_0016 - Assign risk designations	Manual, Disabled	1.1.0 ↗
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 ↗
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	Manual, Disabled	1.1.0 ↗
Protect special information ↗	CMA_0409 - Protect special information	Manual, Disabled	1.1.0 ↗
Rescreen individuals at a defined frequency ↗	CMA_C1512 - Rescreen individuals at a defined frequency	Manual, Disabled	1.1.0 ↗

0106.02a2Organizational.23-02.a 02.01 Prior to Employment

ID: 0106.02a2Organizational.23-02.a 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 ↗
Protect special information ↗	CMA_0409 - Protect special information	Manual, Disabled	1.1.0 ↗
Rescreen individuals at a defined frequency ↗	CMA_C1512 - Rescreen individuals at a defined frequency	Manual, Disabled	1.1.0 ↗

0107.02d1Organizational.1-02.d 02.03 During Employment

ID: 0107.02d1Organizational.1-02.d Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish information security workforce development and improvement program ↗	CMA_C1752 - Establish information security workforce development and improvement program	Manual, Disabled	1.1.0 ↗

0108.02d1Organizational.23-02.d 02.03 During Employment

ID: 0108.02d1Organizational.23-02.d 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 ↗
Implement security testing, training, and monitoring plans ↗	CMA_C1753 - Implement security testing, training, and monitoring plans	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 periodic role-based security training ↗	CMA_C1095 - Provide periodic 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 ↗
Require developers to provide training ↗	CMA_C1611 - Require developers to provide training	Manual, Disabled	1.1.0 ↗
Retain training records ↗	CMA_0456 - Retain training records	Manual, Disabled	1.1.0 ↗
Review security testing, training, and monitoring plans ↗	CMA_C1754 - Review security testing, training, and monitoring plans	Manual, Disabled	1.1.0 ↗

0109.02d1Organizational.4-02.d 02.03 During Employment

ID: 0109.02d1Organizational.4-02.d 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 ↗
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	1.1.0 ↗
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce rules of behavior and access agreements 	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	1.1.0 
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 
Prohibit unfair practices 	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0 
Provide periodic role-based security training 	CMA_C1095 - Provide periodic role-based security training	Manual, Disabled	1.1.0 
Provide periodic security awareness training 	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 
Provide role-based practical exercises 	CMA_C1096 - Provide role-based practical exercises	Manual, Disabled	1.1.0 
Provide role-based security training 	CMA_C1094 - Provide role-based security training	Manual, Disabled	1.1.0 
Provide role-based training on suspicious activities 	CMA_C1097 - Provide role-based training on suspicious activities	Manual, Disabled	1.1.0 
Provide security awareness training for insider threats 	CMA_0417 - Provide security awareness training for insider threats	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 
Review and sign revised rules of behavior 	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 
Update information security policies 	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 
Update rules of behavior and access agreements 	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Update rules of behavior and access agreements every 3 years 	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0 

0110.02d2Organizational.1-02.d 02.03 During Employment

ID: 0110.02d2Organizational.1-02.d 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 
Establish information security workforce development and improvement program 	CMA_C1752 - Establish information security workforce development and improvement program	Manual, Disabled	1.1.0 

0111.02d2Organizational.2-02.d 02.03 During Employment

ID: 0111.02d2Organizational.2-02.d 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	1.1.0 
Establish third-party personnel security requirements 	CMA_C1529 - Establish third-party personnel security requirements	Manual, Disabled	1.1.0 
Monitor third-party provider compliance 	CMA_C1533 - Monitor third-party provider compliance	Manual, Disabled	1.1.0 
Provide periodic security awareness training 	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 
Provide security awareness training for insider threats 	CMA_0417 - Provide security awareness training for insider	Manual, Disabled	1.1.0 

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	threats		
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 ↗
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 ↗

01110.05a1Organizational.5-05.a 05.01 Internal Organization

ID: 01110.05a1Organizational.5-05.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 ↗
Document third-party personnel security requirements ↗	CMA_C1531 - Document third-party personnel security requirements	Manual, Disabled	1.1.0 ↗
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	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 ↗

01111.05a2Organizational.5-05.a 05.01 Internal Organization

ID: 01111.05a2Organizational.5-05.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 ↗

0112.02d2Organizational.3-02.d 02.03 During Employment

ID: 0112.02d2Organizational.3-02.d 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 appropriate usage of all accounts ↗	CMA_C1023 - Enforce appropriate usage of all accounts	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 ↗
Establish usage restrictions for mobile code technologies ↗	CMA_C1652 - Establish usage restrictions for mobile code technologies	Manual, Disabled	1.1.0 ↗
Monitor account activity ↗	CMA_0377 - Monitor account activity	Manual, Disabled	1.1.0 ↗
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 ↗

0113.04a1Organizational.123-04.a 04.01 Information Security Policy

ID: 0113.04a1Organizational.123-04.a Ownership: Shared

[Expand table](#)

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 ↗
Protect the information security program plan ↗	CMA_C1732 - Protect the information security program plan	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗

0114.04b1Organizational.1-04.b 04.01 Information Security Policy

ID: 0114.04b1Organizational.1-04.b 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 ↗
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	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 system and services acquisition policies and procedures ↗	CMA_C1560 - Review and update system and services acquisition policies and procedures	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update system maintenance policies and procedures ↗	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗

0115.04b2Organizational.123-04.b 04.01 Information Security Policy

ID: 0115.04b2Organizational.123-04.b 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 ↗
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	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 ↗

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 ↗
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 ↗
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 ↗

0116.04b3Organizational.1-04.b 04.01 Information Security Policy

ID: 0116.04b3Organizational.1-04.b 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 ↗
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 planning policies and procedures ↗	CMA_C1491 - Review and update planning 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 ↗

0117.05a1Organizational.1-05.a 05.01 Internal Organization

ID: 0117.05a1Organizational.1-05.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 ↗

0118.05a1Organizational.2-05.a 05.01 Internal Organization

ID: 0118.05a1Organizational.2-05.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 and establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	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 ↗
Establish information security workforce development and improvement program ↗	CMA_C1752 - Establish information security workforce development and improvement 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 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗

0119.05a1Organizational.3-05.a 05.01 Internal Organization

ID: 0119.05a1Organizational.3-05.a 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 ↗

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

0120.05a1Organizational.4-05.a 05.01 Internal Organization

ID: 0120.05a1Organizational.4-05.a 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 ↗
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 ↗

0121.05a2Organizational.12-05.a 05.01 Internal Organization

ID: 0121.05a2Organizational.12-05.a 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 ↗
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 ↗
Review and update risk assessment policies and procedures ↗	CMA_C1537 - Review and update risk assessment policies and procedures	Manual, Disabled	1.1.0 ↗

0122.05a2Organizational.3-05.a 05.01 Internal Organization

ID: 0122.05a2Organizational.3-05.a 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 ↗
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 ↗
Provide security training for new users ↗	CMA_0419 - Provide security training for new users	Manual, Disabled	1.1.0 ↗

0123.05a2Organizational.4-05.a 05.01 Internal Organization

ID: 0123.05a2Organizational.4-05.a Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	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 ↗

0124.05a3Organizational.1-05.a 05.01 Internal Organization

ID: 0124.05a3Organizational.1-05.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 ↗
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗

0125.05a3Organizational.2-05.a 05.01 Internal Organization

ID: 0125.05a3Organizational.2-05.a 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 ↗
Assess Security Controls ↗	CMA_C1145 - Assess Security Controls	Manual, Disabled	1.1.0 ↗
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 ↗
Develop security assessment plan ↗	CMA_C1144 - Develop security assessment plan	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 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	1.1.0 ↗

0135.02f1Organizational.56-02.f 02.03 During Employment

ID: 0135.02f1Organizational.56-02.f Ownership: Shared

[] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish information security workforce development and improvement program ↗	CMA_C1752 - Establish information security workforce development and improvement program	Manual, Disabled	1.1.0 ↗
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 ↗
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 ↗

0137.02a1Organizational.3-02.a 02.01 Prior to Employment

ID: 0137.02a1Organizational.3-02.a 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	1.1.0 ↗

0162.04b1Organizational.2-04.b 04.01 Information Security Policy

ID: 0162.04b1Organizational.2-04.b 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 ↗
Review and update information integrity policies and procedures ↗	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	1.1.0 ↗

0165.05a3Organizational.3-05.a 05.01 Internal Organization

ID: 0165.05a3Organizational.3-05.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	1.1.0 ↗

0177.05h1Organizational.12-05.h 05.01 Internal Organization

ID: 0177.05h1Organizational.12-05.h 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 ↗
Assess Security Controls ↗	CMA_C1145 - Assess Security	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Controls	Disabled	
Develop security assessment plan ↗	CMA_C1144 - Develop security assessment plan	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 ↗
Select additional testing for security control assessments ↗	CMA_C1149 - Select additional testing for security control assessments	Manual, Disabled	1.1.0 ↗

0178.05h1Organizational.3-05.h 05.01 Internal Organization

ID: 0178.05h1Organizational.3-05.h 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 ↗
Produce Security Assessment report ↗	CMA_C1146 - Produce Security Assessment report	Manual, Disabled	1.1.0 ↗

0179.05h1Organizational.4-05.h 05.01 Internal Organization

ID: 0179.05h1Organizational.4-05.h 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 plans of action and milestones for security program process ↗	CMA_C1737 - Implement plans of action and milestones for security program process	Manual, Disabled	1.1.0 ↗

0180.05h2Organizational.1-05.h 05.01 Internal Organization

ID: 0180.05h2Organizational.1-05.h 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 ↗

02 Endpoint Protection

0201.09j1Organizational.124-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 0201.09j1Organizational.124-09.j 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	AuditIfNotExists, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	learning to analyze the applications running on each machine and suggest the list of known-safe applications.		
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 ↴
Deploy default Microsoft IaaSAntimalware extension for Windows Server ↴	This policy deploys a Microsoft IaaSAntimalware extension with a default configuration when a VM is not configured with the antimalware extension.	deployIfNotExists	1.1.0 ↴
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 ↴
Document wireless access security controls ↴	CMA_C1695 - Document wireless access security controls	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 ↴
Microsoft Antimalware for Azure should be configured to automatically update protection signatures ↴	This policy audits any Windows virtual machine not configured with automatic update of Microsoft Antimalware protection signatures.	AuditIfNotExists, Disabled	1.0.0 ↴
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 ↴
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 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 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 ↗
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	4.0.0 ↗
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗

0202.09j1Organizational.3-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 0202.09j1Organizational.3-09.j 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	1.1.0 ↗
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 ↗
Govern and monitor audit	CMA_0289 - Govern and monitor	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
processing activities 	audit processing activities	Disabled	
Integrate Audit record analysis 	CMA_C1120 - Integrate Audit record analysis	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 activity	Manual, Disabled	1.1.0 
Review role group changes weekly 	CMA_0476 - Review role group changes weekly	Manual, Disabled	1.1.0 
Specify permitted actions associated with customer audit information 	CMA_C1122 - Specify permitted actions associated with customer audit information	Manual, Disabled	1.1.0 

0204.09j2Organizational.1-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 0204.09j2Organizational.1-09.j 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 🔗
Create alternative actions for identified anomalies 🔗	CMA_C1711 - Create alternative actions for identified anomalies	Manual, Disabled	1.1.0 🔗
Manage gateways 🔗	CMA_0363 - Manage gateways	Manual, Disabled	1.1.0 🔗
Notify personnel of any failed security verification tests 🔗	CMA_C1710 - Notify personnel of any failed security verification tests	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 security function verification at a defined frequency 🔗	CMA_C1709 - Perform security function verification at a defined frequency	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 🔗
Verify security functions 🔗	CMA_C1708 - Verify security functions	Manual, Disabled	1.1.0 🔗

0205.09j2Organizational.2-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 0205.09j2Organizational.2-09.j 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 ↗
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 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	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 ↗
Review threat protection status weekly ↗	CMA_0479 - Review threat protection status weekly	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 ↗
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗

0206.09j2Organizational.34-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 0206.09j2Organizational.34-09.j 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)
	USB		
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 

0207.09j2Organizational.56-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 0207.09j2Organizational.56-09.j 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 
Review threat protection status weekly 	CMA_0479 - Review threat protection status weekly	Manual, Disabled	1.1.0 

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗

0208.09j2Organizational.7-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 0208.09j2Organizational.7-09.j 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 ↗
Employ boundary protection to isolate information systems ↗	CMA_C1639 - Employ boundary protection to isolate information 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 ↗

0209.09m3Organizational.7-09.m 09.06 Network Security Management

ID: 0209.09m3Organizational.7-09.m 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 ↗
Employ automatic shutdown/restart when violations	CMA_C1715 - Employ automatic shutdown/restart when violations are	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
are detected ↗	detected		
Facilitate information sharing ↗	CMA_0284 - Facilitate information sharing	Manual, Disabled	1.1.0 ↗
Record disclosures of PII to third parties ↗	CMA_0422 - Record disclosures of PII to third parties	Manual, Disabled	1.1.0 ↗
Train staff on PII sharing and its consequences ↗	CMA_C1871 - Train staff on PII sharing and its consequences	Manual, Disabled	1.1.0 ↗
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↗

0214.09j1Organizational.6-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 0214.09j1Organizational.6-09.j 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 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege access	Manual, Disabled	1.1.0 ↗
Limit privileges to make changes in production environment ↗	CMA_C1206 - Limit privileges to make changes in production environment	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 ↗

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 ↗
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 ↗

0215.09j2Organizational.8-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 0215.09j2Organizational.8-09.j 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 ↗
Review threat protection status weekly ↗	CMA_0479 - Review threat protection status weekly	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Update antivirus definitions	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0

0216.09j2Organizational.9-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 0216.09j2Organizational.9-09.j 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
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 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

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

0217.09j2Organizational.10-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 0217.09j2Organizational.10-09.j 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
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
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
Manage gateways	CMA_0363 - Manage gateways	Manual, Disabled	1.1.0
Observe and report security weaknesses	CMA_0384 - Observe and report security weaknesses	Manual, Disabled	1.1.0

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 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 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 exploit protection events ↗	CMA_0472 - Review exploit protection events	Manual, Disabled	1.1.0 ↗
Review file and folder activity ↗	CMA_0473 - Review file and folder activity	Manual, Disabled	1.1.0 ↗
Review malware detections report weekly ↗	CMA_0475 - Review malware detections report weekly	Manual, Disabled	1.1.0 ↗
Review role group changes weekly ↗	CMA_0476 - Review role group changes 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 ↗

0219.09j2Organizational.12-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 0219.09j2Organizational.12-09.j 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 ↗
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 ↗

0225.09k1Organizational.1-09.k 09.04 Protection Against Malicious and Mobile Code

ID: 0225.09k1Organizational.1-09.k Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize, monitor, and control usage of mobile code technologies ↗	CMA_C1653 - Authorize, monitor, and control usage of mobile code technologies	Manual, Disabled	1.1.0 ↗
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)
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 ↗
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 ↗
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 ↗

0226.09k1Organizational.2-09.k 09.04 Protection Against Malicious and Mobile Code

ID: 0226.09k1Organizational.2-09.k Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize, monitor, and control usage of mobile code technologies ↗	CMA_C1653 - Authorize, monitor, and control usage of mobile code technologies	Manual, Disabled	1.1.0 ↗
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 ↗
Define acceptable and unacceptable mobile code	CMA_C1651 - Define acceptable and unacceptable mobile code	Manual, Disabled	1.1.0 ↗

Technologies	Description	Effect(s)	Version
(Azure portal) Establish usage restrictions for mobile code technologies ↗	CMA_C1652 - Establish usage restrictions for mobile code technologies	Manual, Disabled	(GitHub) 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 ↗

0227.09k2Organizational.12-09.k 09.04 Protection Against Malicious and Mobile Code

ID: 0227.09k2Organizational.12-09.k Ownership: Shared

[\[\]](#) Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(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 ↗
Authorize, monitor, and control usage of mobile code technologies ↗	CMA_C1653 - Authorize, monitor, and control usage of mobile code technologies	Manual, Disabled	1.1.0 ↗
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 ↗
Define acceptable and unacceptable mobile code technologies ↗	CMA_C1651 - Define acceptable and unacceptable mobile code technologies	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	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 ↗
Establish usage restrictions for mobile code technologies ↗	CMA_C1652 - Establish usage restrictions for mobile code technologies	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 ↗
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	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 ↗
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 ↗
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗

0228.09k2Organizational.3-09.k 09.04 Protection Against Malicious and Mobile Code

ID: 0228.09k2Organizational.3-09.k Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate process to highlight unreviewed change proposals ↗	CMA_C1193 - Automate process to highlight unreviewed change proposals	Manual, Disabled	1.1.0 ↗
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	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 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 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

03 Portable Media Security

0301.09o1Organizational.123-09.o 09.07 Media Handling

ID: 0301.09o1Organizational.123-09.o 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 ↴
Control use of portable storage devices ↴	CMA_0083 - Control use of portable storage devices	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 ↴
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 ↴
Manage the transportation of assets ↴	CMA_0370 - Manage the transportation of assets	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 ↴
Restrict media use ↴	CMA_0450 - Restrict media use	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 ↴
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 ↴

[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 ↗
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 ↗
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: https://aka.ms/disksse , ↗ Different disk encryption offerings: https://aka.ms/diskencryptioncomparison ↗	AuditIfNotExists, Disabled	2.0.3 ↗

0303.09o2Organizational.2-09.o 09.07 Media Handling

ID: 0303.09o2Organizational.2-09.o 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 ↗
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 ↗

0304.09o3Organizational.1-09.o 09.07 Media Handling

ID: 0304.09o3Organizational.1-09.o 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 ↗
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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
to secure all media ↴	media	Disabled	
Require encryption on Data Lake Store accounts ↴	This policy ensures encryption is enabled on all Data Lake Store accounts	deny	1.0.0 ↴
Restrict media use ↴	CMA_0450 - Restrict media use	Manual, Disabled	1.1.0 ↴
SQL managed instances should use customer-managed keys to encrypt data at rest ↴	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	2.0.0 ↴
SQL servers should use customer-managed keys to encrypt data at rest ↴	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	2.0.1 ↴

0305.09q1Organizational.12-09.q 09.07 Media Handling

ID: 0305.09q1Organizational.12-09.q 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	1.1.0 ↴
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 ↴

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 
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 

0306.09q1Organizational.3-09.q 09.07 Media Handling

ID: 0306.09q1Organizational.3-09.q 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 
Ensure authorized users protect provided authenticators 	CMA_C1339 - Ensure authorized users protect provided authenticators	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 
Facilitate information sharing 	CMA_0284 - Facilitate information sharing	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 training for protecting authenticators 	CMA_0329 - Implement training for protecting authenticators	Manual, Disabled	1.1.0 

0307.09q2Organizational.12-09.q 09.07 Media Handling

ID: 0307.09q2Organizational.12-09.q Ownership: Shared

 [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Control information flow 	CMA_0079 - Control information flow	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 

0308.09q3Organizational.1-09.q 09.07 Media Handling

ID: 0308.09q3Organizational.1-09.q 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 
Manage the transportation of assets 	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 

0314.09q3Organizational.2-09.q 09.07 Media Handling

ID: 0314.09q3Organizational.2-09.q 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 
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 

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Determine assertion requirements ↗	CMA_0136 - Determine assertion requirements	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	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 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗
Restrict access to private keys ↗	CMA_0445 - Restrict access to private keys	Manual, Disabled	1.1.0 ↗

04 Mobile Device Security

0401.01x1System.124579-01.x 01.07 Mobile Computing and Teleworking

ID: 0401.01x1System.124579-01.x Ownership: Shared

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize, monitor, and control usage of mobile code technologies ↗	CMA_C1653 - Authorize, monitor, and control usage of mobile code technologies	Manual, Disabled	1.1.0 ↗
Define acceptable and unacceptable mobile code technologies ↗	CMA_C1651 - Define acceptable and unacceptable mobile code technologies	Manual, Disabled	1.1.0 ↗
Define mobile device requirements ↗	CMA_0122 - Define mobile device requirements	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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	1.1.0 ↗
Prohibit remote activation of collaborative computing devices ↗	CMA_C1648 - Prohibit remote activation of collaborative computing devices	Manual, Disabled	1.1.0 ↗
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗

0403.01x1System.8-01.x 01.07 Mobile Computing and Teleworking

ID: 0403.01x1System.8-01.x 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 ↗
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Ensure security safeguards not needed when the individuals return ↗	CMA_C1183 - Ensure security safeguards not needed when the individuals return	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 ↗
Not allow for information systems to accompany with individuals ↗	CMA_C1182 - Not allow for information systems to accompany with individuals	Manual, Disabled	1.1.0 ↗
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗

0405.01y1Organizational.12345678-01.y 01.07 Mobile Computing and Teleworking

ID: 0405.01y1Organizational.12345678-01.y 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 ↗

0407.01y2Organizational.1-01.y 01.07 Mobile Computing and Teleworking

ID: 0407.01y2Organizational.1-01.y 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 ↗
Implement controls to secure alternate work sites ↗	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	1.1.0 ↗

0408.01y3Organizational.12-01.y 01.07 Mobile Computing and Teleworking

ID: 0408.01y3Organizational.12-01.y 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	1.1.0 ↗
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 ↗
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 ↗
Manage nonlocal maintenance and diagnostic activities ↗	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	1.1.0 ↗

0409.01y3Organizational.3-01.y 01.07 Mobile Computing and Teleworking

ID: 0409.01y3Organizational.3-01.y 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 ↗

0410.01x1System.12-01.xMobileComputingandCommunications 01.07 Mobile Computing and Teleworking

ID: 0410.01x1System.12-01.xMobileComputingandCommunications 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 ↗

0415.01y1Organizational.10-01.y 01.07 Mobile Computing and Teleworking

ID: 0415.01y1Organizational.10-01.y 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	1.1.0 ↗
Define mobile device requirements ↗	CMA_0122 - Define mobile device 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 ↗

0416.01y3Organizational.4-01.y 01.07 Mobile Computing and Teleworking

ID: 0416.01y3Organizational.4-01.y 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	1.1.0 ↗
Define mobile device requirements ↗	CMA_0122 - Define mobile device requirements	Manual, Disabled	1.1.0 ↗
Manage nonlocal maintenance and diagnostic activities ↗	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗

0417.01y3Organizational.5-01.y 01.07 Mobile Computing and Teleworking

ID: 0417.01y3Organizational.5-01.y 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 ↗

0425.01x1System.13-01.x 01.07 Mobile Computing and Teleworking

ID: 0425.01x1System.13-01.x 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 ↗

0426.01x2System.1-01.x 01.07 Mobile Computing and Teleworking

ID: 0426.01x2System.1-01.x 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 ↗
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Ensure security safeguards not needed when the individuals return ↗	CMA_C1183 - Ensure security safeguards not needed when the individuals return	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 ↗
Not allow for information systems to accompany with individuals ↗	CMA_C1182 - Not allow for information systems to accompany with individuals	Manual, Disabled	1.1.0 ↗
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗

0427.01x2System.2-01.x 01.07 Mobile Computing and Teleworking

ID: 0427.01x2System.2-01.x 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 ↗
Ensure security safeguards not needed when the individuals return ↗	CMA_C1183 - Ensure security safeguards not needed when the individuals return	Manual, Disabled	1.1.0 ↗
Not allow for information systems to accompany with individuals ↗	CMA_C1182 - Not allow for information systems to accompany with individuals	Manual, Disabled	1.1.0 ↗
Protect data in transit using	CMA_0403 - Protect data in transit	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
encryption ↗	using encryption	Disabled	

0428.01x2System.3-01.x 01.07 Mobile Computing and Teleworking

ID: 0428.01x2System.3-01.x 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 ↗
Ensure security safeguards not needed when the individuals return ↗	CMA_C1183 - Ensure security safeguards not needed when the individuals return	Manual, Disabled	1.1.0 ↗
Not allow for information systems to accompany with individuals ↗	CMA_C1182 - Not allow for information systems to accompany with individuals	Manual, Disabled	1.1.0 ↗
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗

0429.01x1System.14-01.x 01.07 Mobile Computing and Teleworking

ID: 0429.01x1System.14-01.x Ownership: Shared

↔ Expand table

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 ↗
Define mobile device requirements ↗	CMA_0122 - Define mobile device requirements	Manual, Disabled	1.1.0 ↗

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	1.1.0 ↴
Implement controls to secure all media ↴	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↴
Not allow for information systems to accompany with individuals ↴	CMA_C1182 - Not allow for information systems to accompany with individuals	Manual, Disabled	1.1.0 ↴
Protect data in transit using encryption ↴	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↴
Restrict media use ↴	CMA_0450 - Restrict media use	Manual, Disabled	1.1.0 ↴

Identification of Risks Related to External Parties

Access to the organizations information and systems by external parties is not permitted until due diligence has been conducted, the appropriate controls have been implemented, and a contract/agreement reflecting the security requirements is signed acknowledging they understand and accept their obligations.

ID: 1401.05i1Organizational.1239 - 05.i Ownership: Customer

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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	Audit, Deny, Disabled	2.0.0 ↴

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
as man-in-the-middle, eavesdropping, and session-hijacking			

Remote access connections between the organization and external parties are encrypted.

ID: 1402.05i1Organizational.45 - 05.i Ownership: Customer

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

Name	Description	Effect(s)	Version
(Azure portal)		(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 ↴

Access granted to external parties is limited to the minimum necessary and granted only for the duration required.

ID: 1403.05i1Organizational.67 - 05.i Ownership: Customer

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

Name	Description	Effect(s)	Version
(Azure portal)		(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 ↴

The identification of risks related to external party access takes into account a minimal set of specifically defined issues.

ID: 1418.05i1Organizational.8 - 05.i Ownership: Customer

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce SSL connection should be enabled for MySQL database servers ↴	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	1.0.1 ↴

05 Wireless Security

0504.09m2Organizational.5-09.m 09.06 Network Security Management

ID: 0504.09m2Organizational.5-09.m 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 ↴
Document wireless access security controls ↴	CMA_C1695 - Document wireless access security controls	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 ↴

0505.09m2Organizational.3-09.m 09.06 Network Security Management

ID: 0505.09m2Organizational.3-09.m 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 ↗
Define requirements for managing assets ↗	CMA_0125 - Define requirements for managing assets	Manual, Disabled	1.1.0 ↗
Document wireless access security controls ↗	CMA_C1695 - Document wireless access security controls	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 ↗
Install an alarm system ↗	CMA_0338 - Install an alarm system	Manual, Disabled	1.1.0 ↗
Manage a secure surveillance camera system ↗	CMA_0354 - Manage a secure surveillance camera system	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗

06 Configuration Management

0601.06g1Organizational.124-06.g 06.02 Compliance with Security Policies and Standards, and Technical Compliance

ID: 0601.06g1Organizational.124-06.g 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop POA&M ↗	CMA_C1156 - Develop POA&M	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 ↗
Update POA&M items ↗	CMA_C1157 - Update POA&M items	Manual, Disabled	1.1.0 ↗

0602.06g1Organizational.3-06.g 06.02 Compliance with Security Policies and Standards, and Technical Compliance

ID: 0602.06g1Organizational.3-06.g 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 ↗
Deliver security assessment results ↗	CMA_C1147 - Deliver security assessment results	Manual, Disabled	1.1.0 ↗
Develop configuration management plan ↗	CMA_C1232 - Develop configuration management plan	Manual, Disabled	1.1.0 ↗
Develop POA&M ↗	CMA_C1156 - Develop POA&M	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 audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Produce Security Assessment report ↗	CMA_C1146 - Produce Security Assessment report	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 ↗
Update POA&M items ↗	CMA_C1157 - Update POA&M items	Manual, Disabled	1.1.0 ↗

0603.06g2Organizational.1-06.g 06.02 Compliance with Security Policies and Standards, and Technical Compliance

ID: 0603.06g2Organizational.1-06.g 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 ↗
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 ↗
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

0604.06g2Organizational.2-06.g 06.02 Compliance with Security Policies and Standards, and Technical Compliance

ID: 0604.06g2Organizational.2-06.g 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 ↗
Configure detection whitelist ↗	CMA_0068 - Configure detection whitelist	Manual, Disabled	1.1.0 ↗
Develop security assessment plan ↗	CMA_C1144 - Develop security assessment plan	Manual, Disabled	1.1.0 ↗
Employ independent assessors for continuous monitoring ↗	CMA_C1168 - Employ independent assessors for continuous monitoring	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 ↗
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 ↗

0605.10h1System.12-10.h 10.04 Security of System Files

ID: 0605.10h1System.12-10.h 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 ↗
Limit privileges to make changes in production environment ↗	CMA_C1206 - Limit privileges to make changes in production environment	Manual, Disabled	1.1.0 ↗
Review and	CMA_C1207 - Review and reevaluate	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
reevaluate privileges ↗	privileges	Disabled	
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 ↗
Windows machines should meet requirements for 'Security Options - Audit' ↗	Windows machines should have the specified Group Policy settings in the category 'Security Options - Audit' for forcing audit policy subcategory and shutting down if unable to log security audits. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗
Windows machines should meet requirements for 'System Audit Policies - Account Management' ↗	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Account Management' for auditing application, security, and user group management, and other management events. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗

0613.06h1Organizational.12-06.h 06.02 Compliance with Security Policies and Standards, and Technical Compliance

ID: 0613.06h1Organizational.12-06.h 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 ↗

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

0614.06h2Organizational.12-06.h 06.02 Compliance with Security Policies and Standards, and Technical Compliance

ID: 0614.06h2Organizational.12-06.h 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 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗
Select additional testing for security control assessments ↗	CMA_C1149 - Select additional testing for security control assessments	Manual, Disabled	1.1.0 ↗

0615.06h2Organizational.3-06.h 06.02 Compliance with Security Policies and Standards, and Technical Compliance

ID: 0615.06h2Organizational.3-06.h Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Remediate information system flaws 🔗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 

0618.09b1System.1-09.b 09.01 Documented Operating Procedures

ID: 0618.09b1System.1-09.b 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	1.1.0 
Automate implementation of approved change notifications 🔗	CMA_C1196 - Automate implementation of approved change notifications	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 

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
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 manage change integrity ↗	CMA_C1595 - Require developers to manage change integrity	Manual, Disabled	1.1.0 ↗
Retain previous versions of baseline configs ↗	CMA_C1181 - Retain previous versions of baseline configs	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

0626.10h1System.3-10.h 10.04 Security of System Files

ID: 0626.10h1System.3-10.h Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ automatic shutdown/restart when violations are detected ↗	CMA_C1715 - Employ automatic shutdown/restart when violations are detected	Manual, Disabled	1.1.0 ↗
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

0627.10h1System.45-10.h 10.04 Security of System Files

ID: 0627.10h1System.45-10.h 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 ↗
Ensure security safeguards not needed when the individuals return ↗	CMA_C1183 - Ensure security safeguards not needed when the individuals return	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 ↗
Not allow for information systems to accompany with individuals ↗	CMA_C1182 - Not allow for information systems to accompany with individuals	Manual, Disabled	1.1.0 ↗
Retain previous versions of baseline configs ↗	CMA_C1181 - Retain previous versions of baseline configs	Manual, Disabled	1.1.0 ↗
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

0628.10h1System.6-10.h 10.04 Security of System Files

ID: 0628.10h1System.6-10.h Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ automatic shutdown/restart when violations are detected ↗	CMA_C1715 - Employ automatic shutdown/restart when violations are detected	Manual, Disabled	1.1.0 ↗
Incorporate flaw remediation into configuration management ↗	CMA_C1671 - Incorporate flaw remediation into configuration management	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↗

0635.10k1Organizational.12-10.k 10.05 Security In Development and Support Processes

ID: 0635.10k1Organizational.12-10.k Ownership: Shared

↔ Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Incorporate flaw remediation into configuration management ↗	CMA_C1671 - Incorporate flaw remediation into configuration management	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 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗
Review development process, standards and tools ↗	CMA_C1610 - Review development process, standards and tools	Manual, Disabled	1.1.0 ↗
Review malware detections report	CMA_0475 - Review malware detections report weekly	Manual, Disabled	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal) Review threat protection status weekly ↗	CMA_0479 - Review threat protection status weekly	Manual, Disabled	(GitHub) 1.1.0 ↗
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗
Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking' ↗	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Detailed Tracking' for auditing DPAPI, process creation/termination, RPC events, and PNP activity. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗

0636.10k2Organizational.1-10.k 10.05 Security In Development and Support Processes

ID: 0636.10k2Organizational.1-10.k Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Create configuration plan protection ↗	CMA_C1233 - Create configuration plan protection	Manual, Disabled	1.1.0 ↗
Develop and maintain baseline configurations ↗	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	1.1.0 ↗
Develop configuration item identification plan ↗	CMA_C1231 - Develop configuration item identification plan	Manual, Disabled	1.1.0 ↗
Develop configuration management plan ↗	CMA_C1232 - Develop configuration management plan	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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	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 ↗
Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking' ↗	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Detailed Tracking' for auditing DPAPI, process creation/termination, RPC events, and PNP activity. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗

0637.10k2Organizational.2-10.k 10.05 Security In Development and Support Processes

ID: 0637.10k2Organizational.2-10.k Ownership: Shared

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Create configuration plan protection ↗	CMA_C1233 - Create configuration plan protection	Manual, Disabled	1.1.0 ↗
Develop and maintain baseline configurations ↗	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	1.1.0 ↗
Develop configuration item identification plan ↗	CMA_C1231 - Develop configuration item identification plan	Manual, Disabled	1.1.0 ↗
Develop configuration management plan ↗	CMA_C1232 - Develop configuration management plan	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking' ↗	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Detailed Tracking' for auditing DPAPI, process creation/termination, RPC events, and PNP activity. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗

0638.10k2Organizational.34569-10.k 10.05 Security In Development and Support Processes

ID: 0638.10k2Organizational.34569-10.k Ownership: Shared

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

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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
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 ↗
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 ↗
Windows machines should meet requirements for 'System Audit'	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Detailed Tracking' for auditing DPAPI, process creation/termination, RPC events, and PNP	AuditIfExists, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Policies - Detailed Tracking	activity. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol .		

0639.10k2Organizational.78-10.k 10.05 Security In Development and Support Processes

ID: 0639.10k2Organizational.78-10.k 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
Remediate information system flaws	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking' ↗	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Detailed Tracking' for auditing DPAPI, process creation/termination, RPC events, and PNP activity. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗

0640.10k2Organizational.1012-10.k 10.05 Security In Development and Support Processes

ID: 0640.10k2Organizational.1012-10.k 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 ↗
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 ↗
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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
requirements for developers ↗			
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 ↗
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 manage change integrity ↗	CMA_C1595 - Require developers to manage change integrity	Manual, Disabled	1.1.0 ↗
Require developers to produce evidence of security assessment plan execution ↗	CMA_C1602 - Require developers to produce evidence of security assessment plan execution	Manual, Disabled	1.1.0 ↗
Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking' ↗	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Detailed Tracking' for auditing DPAPI, process creation/termination, RPC events, and PNP activity. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗

0641.10k2Organizational.11-10.k 10.05 Security In Development and Support Processes

ID: 0641.10k2Organizational.11-10.k 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 establish a system security plan ↗	CMA_0151 - Develop and establish a system security plan	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 developers ↗	CMA_0270 - Establish configuration management requirements for developers	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 ↗
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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review development process, standards and tools ↗	CMA_C1610 - Review development process, standards and tools	Manual, Disabled	1.1.0 ↗
Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking' ↗	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Detailed Tracking' for auditing DPAPI, process creation/termination, RPC events, and PNP activity. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗

0642.10k3Organizational.12-10.k 10.05 Security In Development and Support Processes

ID: 0642.10k3Organizational.12-10.k 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	1.1.0 ↗
Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking' ↗	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Detailed Tracking' for auditing DPAPI, process creation/termination, RPC events, and PNP activity. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗

0643.10k3Organizational.3-10.k 10.05 Security In Development and Support Processes

ID: 0643.10k3Organizational.3-10.k 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 ↗
Configure actions for noncompliant devices ↗	CMA_0062 - Configure actions for noncompliant devices	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 ↗
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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish a configuration control board ↗	CMA_0254 - Establish a configuration control board	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 a configuration management plan ↗	CMA_0264 - Establish and document a configuration management 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 ↗
Implement an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	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 ↗
Retain previous versions of baseline configs ↗	CMA_C1181 - Retain previous versions of baseline configs	Manual, Disabled	1.1.0 ↗
Windows machines should meet	Windows machines should have the specified Group Policy settings in the	AuditIfNotExists, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
requirements for 'System Audit Policies - Detailed Tracking' ↗	category 'System Audit Policies - Detailed Tracking' for auditing DPAPI, process creation/termination, RPC events, and PNP activity. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗ .		

0644.10k3Organizational.4-10.k 10.05 Security In Development and Support Processes

ID: 0644.10k3Organizational.4-10.k Ownership: Shared

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign account managers ↗	CMA_0015 - Assign account managers	Manual, Disabled	1.1.0 ↗
Audit user account status ↗	CMA_0020 - Audit user account status	Manual, Disabled	1.1.0 ↗
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 ↗
Define information system account types ↗	CMA_0121 - Define information system account types	Manual, Disabled	1.1.0 ↗
Develop configuration item identification plan ↗	CMA_C1231 - Develop configuration item identification plan	Manual, Disabled	1.1.0 ↗
Develop configuration management plan ↗	CMA_C1232 - Develop configuration management plan	Manual, Disabled	1.1.0 ↗
Document access privileges ↗	CMA_0186 - Document access privileges	Manual, Disabled	1.1.0 ↗
Enforce security configuration	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗

settings ↗	Name	Description	Effect(s)	Version
(Azure portal) Establish conditions for role membership ↗	CMA_0269 - Establish conditions for role membership	Manual, Disabled	(GitHub) 1.1.0 ↗	
Govern compliance of cloud service providers ↗	CMA_0290 - Govern compliance of cloud service providers	Manual, Disabled		1.1.0 ↗
Monitor account activity ↗	CMA_0377 - Monitor account activity	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 ↗
Reissue authenticators for changed groups and accounts ↗	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled		1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	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 user accounts ↗	CMA_0480 - Review user accounts	Manual, Disabled		1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled		1.1.0 ↗
Windows machines should meet requirements for 'System Audit Policies - Detailed Tracking' ↗	Windows machines should have the specified Group Policy settings in the category 'System Audit Policies - Detailed Tracking' for auditing DPAPI, process creation/termination, RPC events, and PNP activity. This policy requires that the Guest Configuration prerequisites have been deployed to the	AuditIfNotExists, Disabled		3.0.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
policy assignment scope. For details, visit https://aka.ms/gcpol .			

0662.09sCSPOrganizational.2-09.s 09.08 Exchange of Information

ID: 0662.09sCSPOrganizational.2-09.s Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
App Service apps should have Client Certificates (Incoming client certificates) enabled	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	1.0.0
Employ independent assessors to conduct security control assessments	CMA_C1148 - Employ independent assessors to conduct security control assessments	Manual, Disabled	1.1.0
Select additional testing for security control assessments	CMA_C1149 - Select additional testing for security control assessments	Manual, Disabled	1.1.0

0663.10h1System.7-10.h 10.04 Security of System Files

ID: 0663.10h1System.7-10.h Ownership: Shared

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

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

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 ↗
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↗
Document wireless access security controls ↗	CMA_C1695 - Document wireless access security controls	Manual, Disabled	1.1.0 ↗
Employ automatic shutdown/restart when violations are detected ↗	CMA_C1715 - Employ automatic shutdown/restart when violations are detected	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 ↗
Perform a trend analysis on threats ↗	CMA_0389 - Perform a trend analysis on threats	Manual, Disabled	1.1.0 ↗
Remediate information system flaws ↗	CMA_0427 - Remediate information system flaws	Manual, Disabled	1.1.0 ↗
Review audit data ↗	CMA_0466 - Review audit data	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 ↗
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

0669.10hCSPSystem.1-10.h 10.04 Security of System Files

ID: 0669.10hCSPSystem.1-10.h 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 ↗
Configure actions for noncompliant devices ↗	CMA_0062 - Configure actions for noncompliant devices	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 baseline configurations ↗	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	1.1.0 ↗
Develop configuration item identification plan ↗	CMA_C1231 - Develop configuration item identification plan	Manual, Disabled	1.1.0 ↗
Develop configuration management plan ↗	CMA_C1232 - Develop configuration management plan	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 configuration control board ↗	CMA_0254 - Establish a configuration control board	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 a configuration management plan ↗	CMA_0264 - Establish and document a configuration management 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 ↗
Implement an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗
Require developers to manage change integrity ↗	CMA_C1595 - Require developers to manage change integrity	Manual, Disabled	1.1.0 ↗

0670.10hCSPSystem.2-10.h 10.04 Security of System Files

ID: 0670.10hCSPSystem.2-10.h 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 ↗
Perform disposition review ↗	CMA_0391 - Perform disposition review	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 ↗

0671.10k1System.1-10.k 10.05 Security In Development and Support Processes

ID: 0671.10k1System.1-10.k 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 implementation of approved change notifications ↗	CMA_C1196 - Automate implementation of approved change notifications	Manual, Disabled	1.1.0 ↗
Automate process to highlight unreviewed change proposals ↗	CMA_C1193 - Automate process to highlight unreviewed change	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	proposals		
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 ↗
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 ↗
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	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 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 ↗
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 ↗

0672.10k3System.5-10.k 10.05 Security In Development and Support Processes

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 ↗
Employ automatic shutdown/restart when violations are detected ↗	CMA_C1715 - Employ automatic shutdown/restart when violations are detected	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 ↗
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 ↗
Prohibit binary/machine-executable code ↗	CMA_C1717 - Prohibit binary/machine-executable code	Manual, Disabled	1.1.0 ↗
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

068.06g2Organizational.34-06.g 06.02 Compliance with Security Policies and Standards, and Technical Compliance

ID: 068.06g2Organizational.34-06.g 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 ↗
Employ independent assessors for continuous monitoring ↗	CMA_C1168 - Employ independent assessors for continuous monitoring	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 ↗
Produce Security Assessment report ↗	CMA_C1146 - Produce Security Assessment report	Manual, Disabled	1.1.0 ↗

069.06g2Organizational.56-06.g 06.02 Compliance with Security Policies and Standards, and Technical Compliance

ID: 069.06g2Organizational.56-06.g 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 ↗
Configure detection whitelist ↗	CMA_0068 - Configure detection	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	whitelist	Disabled	
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	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 ↗

07 Vulnerability Management

0701.07a1Organizational.12-07.a 07.01 Responsibility for Assets

ID: 0701.07a1Organizational.12-07.a 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 ↗
Create a data inventory ↗	CMA_0096 - Create a data inventory	Manual, Disabled	1.1.0 ↗
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	1.1.0 ↗
Establish and maintain an asset inventory ↗	CMA_0266 - Establish and maintain an asset inventory	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 ↗
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	1.1.0 ↗

0702.07a1Organizational.3-07.a 07.01 Responsibility for Assets

ID: 0702.07a1Organizational.3-07.a 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 ↗
Establish terms and conditions for processing resources ↗	CMA_C1077 - Establish terms and conditions for processing resources	Manual, Disabled	1.1.0 ↗

0703.07a2Organizational.1-07.a 07.01 Responsibility for Assets

ID: 0703.07a2Organizational.1-07.a Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Maintain records of processing of personal data ↗	CMA_0353 - Maintain records of processing of personal data	Manual, Disabled	1.1.0 ↗

0704.07a3Organizational.12-07.a 07.01 Responsibility for Assets

ID: 0704.07a3Organizational.12-07.a Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Maintain records of processing of personal data ↗	CMA_0353 - Maintain records of processing of personal data	Manual, Disabled	1.1.0 ↗

0705.07a3Organizational.3-07.a 07.01 Responsibility for Assets

ID: 0705.07a3Organizational.3-07.a 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 ↗

0706.10b1System.12-10.b 10.02 Correct Processing in Applications

ID: 0706.10b1System.12-10.b 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Perform information input validation ↗	CMA_C1723 - Perform information input validation	Manual, Disabled	1.1.0 ↗

0708.10b2System.2-10.b 10.02 Correct Processing in Applications

ID: 0708.10b2System.2-10.b Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update information integrity policies and procedures ↗	CMA_C1667 - Review and update information integrity policies and procedures	Manual, Disabled	1.1.0 ↗
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

0709.10m1Organizational.1-10.m 10.06 Technical Vulnerability Management

ID: 0709.10m1Organizational.1-10.m Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
A vulnerability assessment solution should be	Audits virtual machines to detect whether they are running a supported vulnerability assessment solution. A core component of	AuditIfNotExists, Disabled	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
enabled on your virtual machines ↗	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.		
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 ↗
Select additional testing for security control assessments ↗	CMA_C1149 - Select additional testing for security control assessments	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 ↗
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 ↗
Vulnerabilities in security configuration on your virtual machine scale sets	Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks.	AuditIfNotExists, Disabled	3.0.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
should be remediated ↴			
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	1.0.1 ↴
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	3.0.0 ↴
Windows machines should meet requirements for 'Security Options - Microsoft Network Server' ↴	Windows machines should have the specified Group Policy settings in the category 'Security Options - Microsoft Network Server' for disabling SMB v1 server. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↴.	AuditIfNotExists, Disabled	3.0.0 ↴

0710.10m2Organizational.1-10.m 10.06 Technical Vulnerability Management

ID: 0710.10m2Organizational.1-10.m Ownership: Shared

Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(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	CMA_0254 - Establish a configuration control board	Manual, Disabled	1.1.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
board ↗			
Establish and document a configuration management plan ↗	CMA_0264 - Establish and document a configuration management plan	Manual, Disabled	1.1.0 ↗
Govern compliance of cloud service providers ↗	CMA_0290 - Govern compliance of cloud service providers	Manual, Disabled	1.1.0 ↗
Implement an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗
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	1.0.1 ↗

0711.10m2Organizational.23-10.m 10.06 Technical Vulnerability Management

ID: 0711.10m2Organizational.23-10.m 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 ↗

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 ↴

0712.10m2Organizational.4-10.m 10.06 Technical Vulnerability Management

ID: 0712.10m2Organizational.4-10.m 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 ↴
Select additional testing for security control assessments ↴	CMA_C1149 - Select additional testing for security control assessments	Manual, Disabled	1.1.0 ↴

0713.10m2Organizational.5-10.m 10.06 Technical Vulnerability Management

ID: 0713.10m2Organizational.5-10.m Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate flaw remediation ↴	CMA_0027 - Automate flaw remediation	Manual, Disabled	1.1.0 ↴
Establish benchmarks for flaw remediation ↴	CMA_C1675 - Establish benchmarks for flaw remediation	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	1.1.0 ↗
Measure the time between flaw identification and flaw remediation ↗	CMA_C1674 - Measure the time between flaw identification and flaw remediation	Manual, Disabled	1.1.0 ↗
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 ↗

0714.10m2Organizational.7-10.m 10.06 Technical Vulnerability Management

ID: 0714.10m2Organizational.7-10.m 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 ↗
Implement privileged access for executing vulnerability scanning activities ↗	CMA_C1555 - Implement privileged access for executing vulnerability scanning activities	Manual, Disabled	1.1.0 ↗
Integrate audit review, analysis, and reporting ↗	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version
			(GitHub)
Integrate cloud app security with a siem ↗	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	1.1.0 ↗
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 ↗
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 exploit protection events ↗	CMA_0472 - Review exploit protection 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 ↗
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	3.0.0 ↗

0715.10m2Organizational.8-10.m 10.06 Technical Vulnerability Management

ID: 0715.10m2Organizational.8-10.m Ownership: Shared

[Expand table](#)

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

0716.10m3Organizational.1-10.m 10.06 Technical Vulnerability Management

ID: 0716.10m3Organizational.1-10.m 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 ↴
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 ↴

0717.10m3Organizational.2-10.m 10.06 Technical Vulnerability Management

ID: 0717.10m3Organizational.2-10.m 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 threat modeling ↗	CMA_0392 - Perform threat modeling	Manual, Disabled	1.1.0 ↗
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	3.0.0 ↗

0718.10m3Organizational.34-10.m 10.06 Technical Vulnerability Management

ID: 0718.10m3Organizational.34-10.m Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate flaw remediation ↗	CMA_0027 - Automate flaw remediation	Manual, Disabled	1.1.0 ↗
Observe and report security weaknesses ↗	CMA_0384 - Observe and report security weaknesses	Manual, Disabled	1.1.0 ↗
Perform threat modeling ↗	CMA_0392 - Perform threat modeling	Manual, Disabled	1.1.0 ↗
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 ↗

0719.10m3Organizational.5-10.m 10.06 Technical Vulnerability Management

ID: 0719.10m3Organizational.5-10.m 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 threat modeling ↗	CMA_0392 - Perform threat modeling	Manual, Disabled	1.1.0 ↗
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	1.0.1 ↗

0720.07a1Organizational.4-07.a 07.01 Responsibility for Assets

ID: 0720.07a1Organizational.4-07.a Ownership: Shared

[\[\] Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Create a data inventory ↗	CMA_0096 - Create a data inventory	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 ↗

0722.07a1Organizational.67-07.a 07.01 Responsibility for Assets

ID: 0722.07a1Organizational.67-07.a 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Restrict use of open source software ↗	CMA_C1237 - Restrict use of open source software	Manual, Disabled	1.1.0 ↗
Track software license usage ↗	CMA_C1235 - Track software license usage	Manual, Disabled	1.1.0 ↗

0723.07a1Organizational.8-07.a 07.01 Responsibility for Assets

ID: 0723.07a1Organizational.8-07.a 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 ↗

0724.07a3Organizational.4-07.a 07.01 Responsibility for Assets

ID: 0724.07a3Organizational.4-07.a Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enable detection of network devices ↗	CMA_0220 - Enable detection of network devices	Manual, Disabled	1.1.0 ↗
Manage gateways ↗	CMA_0363 - Manage gateways	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 ↗

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 ↗
Update antivirus definitions ↗	CMA_0517 - Update antivirus definitions	Manual, Disabled	1.1.0 ↗

0725.07a3Organizational.5-07.a 07.01 Responsibility for Assets

ID: 0725.07a3Organizational.5-07.a Ownership: Shared

[] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Maintain records of processing of personal data ↗	CMA_0353 - Maintain records of processing of personal data	Manual, Disabled	1.1.0 ↗

0733.10b2System.4-10.b 10.02 Correct Processing in Applications

ID: 0733.10b2System.4-10.b 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 ↗
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↗

0786.10m2Organizational.13-10.m 10.06 Technical Vulnerability Management

ID: 0786.10m2Organizational.13-10.m Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Incorporate flaw remediation into configuration management ↗	CMA_C1671 - Incorporate flaw remediation into configuration management	Manual, Disabled	1.1.0 ↗

0787.10m2Organizational.14-10.m 10.06 Technical Vulnerability Management

ID: 0787.10m2Organizational.14-10.m Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate flaw remediation ↗	CMA_0027 - Automate flaw remediation	Manual, Disabled	1.1.0 ↗
Establish benchmarks for flaw remediation ↗	CMA_C1675 - Establish benchmarks for flaw remediation	Manual, Disabled	1.1.0 ↗
Incorporate flaw remediation into configuration management ↗	CMA_C1671 - Incorporate flaw remediation into configuration management	Manual, Disabled	1.1.0 ↗
Measure the time between flaw identification and flaw remediation ↗	CMA_C1674 - Measure the time between flaw identification and flaw remediation	Manual, Disabled	1.1.0 ↗

0788.10m3Organizational.20-10.m 10.06 Technical Vulnerability Management

ID: 0788.10m3Organizational.20-10.m 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 ↗

0790.10m3Organizational.22-10.m 10.06 Technical Vulnerability Management

ID: 0790.10m3Organizational.22-10.m 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 ↗
Observe and report security weaknesses ↗	CMA_0384 - Observe and report security weaknesses	Manual, Disabled	1.1.0 ↗
Perform threat modeling ↗	CMA_0392 - Perform threat modeling	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 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 exploit protection events ↗	CMA_0472 - Review exploit protection 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 ↗

0791.10b2Organizational.4-10.b 10.02 Correct Processing in Applications

ID: 0791.10b2Organizational.4-10.b 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 ↗
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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↗

08 Network Protection

0805.01m1Organizational.12-01.m 01.04 Network Access Control

ID: 0805.01m1Organizational.12-01.m Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Container Registry should use a virtual network service endpoint ↗	This policy audits any Container Registry not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0-preview ↗
App Service apps should use a virtual network service endpoint ↗	Use virtual network service endpoints to restrict access to your app from selected subnets from an Azure virtual network. To learn more about App Service service endpoints, visit https://aka.ms/appservice-vnet-service-endpoint ↗ .	AuditIfNotExists, Disabled	2.0.1 ↗
Cosmos DB should use a virtual network service endpoint ↗	This policy audits any Cosmos DB not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0 ↗
Event Hub should use a virtual network service endpoint ↗	This policy audits any Event Hub not configured to use a virtual network service endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Gateway subnets should not be configured with a network security group ↗	This policy denies if a gateway subnet is configured with a network security group. Assigning a network security group to a gateway subnet will cause the gateway to stop functioning.	deny	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 ↗	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 https://aka.ms/nsrg-doc ↗	AuditIfNotExists, Disabled	3.0.0 ↗
Key Vault should use a virtual network service endpoint ↗	This policy audits any Key Vault not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0 ↗
SQL Server should use a virtual network service endpoint ↗	This policy audits any SQL Server not configured to use a virtual network service endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗
Storage Accounts should use a virtual network service endpoint ↗	This policy audits any Storage Account not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0 ↗
Subnets should be associated with a Network Security Group ↗	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 ↗
Virtual machines should be connected to an approved virtual network ↗	This policy audits any virtual machine connected to a virtual network that is not approved.	Audit, Deny, Disabled	1.0.0 ↗

0806.01m2Organizational.12356-01.m 01.04 Network Access Control

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Container Registry should use a virtual network service endpoint ↗	This policy audits any Container Registry not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0-preview ↗
App Service apps should use a virtual network service endpoint ↗	Use virtual network service endpoints to restrict access to your app from selected subnets from an Azure virtual network. To learn more about App Service service endpoints, visit https://aka.ms/appservice-vnet-service-endpoint ↗.	AuditIfNotExists, Disabled	2.0.1 ↗
Cosmos DB should use a virtual network service endpoint ↗	This policy audits any Cosmos DB not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0 ↗
Event Hub should use a virtual network service endpoint ↗	This policy audits any Event Hub not configured to use a virtual network service endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗
Gateway subnets should not be configured with a network security group ↗	This policy denies if a gateway subnet is configured with a network security group. Assigning a network security group to a gateway subnet will cause the gateway to stop functioning.	deny	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 ↗	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 https://aka.ms/nsgr-doc ↗	AuditIfNotExists, Disabled	3.0.0 ↗
Isolate SecurID systems, Security Incident	CMA_C1636 - Isolate SecurID systems, Security Incident Management systems	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Management systems ↗			
Key Vault should use a virtual network service endpoint ↗	This policy audits any Key Vault not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0 ↗
SQL Server should use a virtual network service endpoint ↗	This policy audits any SQL Server not configured to use a virtual network service endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗
Storage Accounts should use a virtual network service endpoint ↗	This policy audits any Storage Account not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0 ↗
Subnets should be associated with a Network Security Group ↗	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 ↗
Virtual machines should be connected to an approved virtual network ↗	This policy audits any virtual machine connected to a virtual network that is not approved.	Audit, Deny, Disabled	1.0.0 ↗

0808.10b2System.3-10.b 10.02 Correct Processing in Applications

ID: 0808.10b2System.3-10.b 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 ↗
Route traffic through authenticated proxy network ↗	CMA_C1633 - Route traffic through authenticated proxy network	Manual, Disabled	1.1.0 ↗

0809.01n2Organizational.1234-01.n 01.04 Network Access Control

ID: 0809.01n2Organizational.1234-01.n Ownership: Shared

[+] [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	3.0.0 ↴
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 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 ↴
Authorize, monitor, and control voip ↴	CMA_0025 - Authorize, monitor, and control voip	Manual, Disabled	1.1.0 ↴
Enforce SSL connection should be enabled for MySQL database servers ↴	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	1.0.1 ↴
Enforce SSL connection should be enabled for	Azure Database for PostgreSQL supports connecting your Azure Database for PostgreSQL server to client applications using Secure Sockets Layer (SSL).	Audit, Disabled	1.0.1 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
PostgreSQL database servers ↗	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.		
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 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 ↗
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 ↗
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 https://aka.ms/nsgr-doc ↗	AuditIfNotExists, Disabled	3.0.0 ↗
Manage gateways ↗	CMA_0363 - Manage gateways	Manual, Disabled	1.1.0 ↗
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 ↗
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	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 ↗
Subnets should be associated with a Network Security Group ↗	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 ↗
Virtual machines should be connected to an approved virtual network ↗	This policy audits any virtual machine connected to a virtual network that is not approved.	Audit, Deny, Disabled	1.0.0 ↗

0810.01n2Organizational.5-01.n 01.04 Network Access Control

ID: 0810.01n2Organizational.5-01.n Ownership: Shared

[\[\]](#) 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	3.0.0 ↗
App Service apps should only be	Use of HTTPS ensures server/service authentication and protects data in transit	Audit, Disabled, Deny	4.0.0 ↗

Name	Description	Effect(s)	Version
(Azure portal) App Service apps should use the latest TLS version	from network layer eavesdropping attacks. 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
Configure workstations to check for digital certificates	CMA_0073 - Configure workstations to check for digital certificates	Manual, Disabled	1.1.0
Define cryptographic use	CMA_0120 - Define cryptographic use	Manual, Disabled	1.1.0
Enforce SSL connection should be enabled for MySQL database servers	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	1.0.1
Enforce SSL connection should be enabled for PostgreSQL database servers	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	1.0.1
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 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	AuditIfNotExists, Disabled	2.0.1

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	for Function apps to take advantage of security fixes, if any, and/or new functionalities of the latest version.		
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 https://aka.ms/nsg-doc ↗</p>	AuditIfNotExists, Disabled	3.0.0 ↗
Only secure connections to your Azure Cache for Redis should be enabled ↗	<p>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</p>	Audit, Deny, Disabled	1.0.0 ↗
Produce, control and distribute asymmetric cryptographic keys ↗	<p>CMA_C1646 - Produce, control and distribute asymmetric cryptographic keys</p>	Manual, Disabled	1.1.0 ↗
Protect data in transit using encryption ↗	<p>CMA_0403 - Protect data in transit using encryption</p>	Manual, Disabled	1.1.0 ↗
Protect passwords with encryption ↗	<p>CMA_0408 - Protect passwords with encryption</p>	Manual, Disabled	1.1.0 ↗
Secure transfer to storage accounts should be enabled ↗	<p>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</p>	Audit, Deny, Disabled	2.0.0 ↗
Subnets should be associated with a Network Security Group ↗	<p>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.</p>	AuditIfNotExists, Disabled	3.0.0 ↗
Virtual machines should be connected	<p>This policy audits any virtual machine connected to a virtual network that is not</p>	Audit, Deny, Disabled	1.0.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
to an approved virtual network ↗	approved.		

08101.09m2Organizational.14-09.m 09.06 Network Security Management

ID: 08101.09m2Organizational.14-09.m Ownership: Shared

[\[\] Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Configure workstations to check for digital certificates ↗	CMA_0073 - Configure workstations to check for digital certificates	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 ↗
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	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 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	Manual, Disabled	1.1.0 ↗

08102.09nCSPOrganizational.1-09.n 09.06 Network Security Management

ID: 08102.09nCSPOrganizational.1-09.n 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 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	Manual, Disabled	1.1.0 ↗

0811.01n2Organizational.6-01.n 01.04 Network Access Control

ID: 0811.01n2Organizational.6-01.n Ownership: Shared

[\[\]](#) 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	3.0.0 ↗
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 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 ↗
Authorize, monitor, and control voip ↗	CMA_0025 - Authorize, monitor, and control voip	Manual, Disabled	1.1.0 ↗
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	1.1.0 ↗
Determine information protection needs ↗	CMA_C1750 - Determine information protection needs	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ flow control mechanisms of encrypted information ↗	CMA_0211 - Employ flow control mechanisms of encrypted information	Manual, Disabled	1.1.0 ↗
Enforce SSL connection should be enabled for MySQL database servers ↗	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	1.0.1 ↗
Enforce SSL connection should be enabled for PostgreSQL database servers ↗	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	1.0.1 ↗
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 ↗
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 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	AuditIfNotExists, Disabled	2.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	for Function apps to take advantage of security fixes, if any, and/or new functionalities of the latest version.		
Identify and manage downstream information exchanges ↗	CMA_0298 - Identify and manage downstream information exchanges	Manual, Disabled	1.1.0 ↗
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 ↗
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 https://aka.ms/nsgr-doc ↗	AuditIfNotExists, Disabled	3.0.0 ↗
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 ↗
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	1.1.0 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	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	Audit, Deny, Disabled	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking		
Subnets should be associated with a Network Security Group ↗	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 ↗
Virtual machines should be connected to an approved virtual network ↗	This policy audits any virtual machine connected to a virtual network that is not approved.	Audit, Deny, Disabled	1.0.0 ↗

0812.01n2Organizational.8-01.n 01.04 Network Access Control

ID: 0812.01n2Organizational.8-01.n Ownership: Shared

[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	3.0.0 ↗
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 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce SSL connection should be enabled for MySQL database servers ↗	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	1.0.1 ↗
Enforce SSL connection should be enabled for PostgreSQL database servers ↗	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	1.0.1 ↗
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 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 ↗
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 https://aka.ms/nsgr-doc ↗	AuditIfNotExists, Disabled	3.0.0 ↗
Only secure connections to your	Audit enabling of only connections via SSL to Azure Cache for Redis. Use of secure connections ensures authentication	Audit, Deny, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Cache for Redis should be enabled ↴	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		
Prevent split tunneling for remote devices ↴	CMA_C1632 - Prevent split tunneling for remote devices	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 ↴
Subnets should be associated with a Network Security Group ↴	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 ↴
Virtual machines should be connected to an approved virtual network ↴	This policy audits any virtual machine connected to a virtual network that is not approved.	Audit, Deny, Disabled	1.0.0 ↴

0814.01n1Organizational.12-01.n 01.04 Network Access Control

ID: 0814.01n1Organizational.12-01.n Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adaptive network hardening recommendations should be applied on	Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security	AuditIfNotExists, Disabled	3.0.0 ↴

Name	Description	Effect(s)	Version
(Azure portal)	(GitHub)		
internet facing virtual machines ↗	Group rule recommendations that reduce the potential attack surface		
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 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 ↗
Enforce SSL connection should be enabled for MySQL database servers ↗	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	1.0.1 ↗
Enforce SSL connection should be enabled for PostgreSQL database servers ↗	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	1.0.1 ↗
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 use the latest TLS version ↗	Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance	AuditIfNotExists, Disabled	2.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	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.		
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 https://aka.ms/nsg-doc ↗	AuditIfNotExists, Disabled	3.0.0 ↗
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 ↗
Subnets should be associated with a Network Security Group ↗	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 ↗
Virtual machines should be connected to an approved virtual network ↗	This policy audits any virtual machine connected to a virtual network that is not approved.	Audit, Deny, Disabled	1.0.0 ↗

0815.01o2Organizational.123-01.o 01.04 Network Access Control

ID: 0815.01o2Organizational.123-01.o 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 ↗
Route traffic through authenticated proxy network ↗	CMA_C1633 - Route traffic through authenticated proxy network	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 ↗

0816.01w1System.1-01.w 01.06 Application and Information Access Control

ID: 0816.01w1System.1-01.w 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 ↗
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 ↗

0817.01w2System.123-01.w 01.06 Application and Information Access Control

[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 ↗
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	1.1.0 ↗
Employ boundary protection to isolate information systems ↗	CMA_C1639 - Employ boundary protection to isolate information systems	Manual, Disabled	1.1.0 ↗
Ensure system capable of dynamic isolation of resources ↗	CMA_C1638 - Ensure system capable of dynamic isolation of resources	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 system boundary protection ↗	CMA_0328 - Implement system boundary protection	Manual, Disabled	1.1.0 ↗
Isolate SecurID systems, Security Incident Management systems ↗	CMA_C1636 - Isolate SecurID systems, Security Incident Management systems	Manual, Disabled	1.1.0 ↗
Maintain separate execution domains for running processes ↗	CMA_C1665 - Maintain separate execution domains for running processes	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 ↗

0818.01w3System.12-01.w 01.06 Application and Information Access Control

ID: 0818.01w3System.12-01.w 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 ↗
Maintain separate execution domains for running processes ↗	CMA_C1665 - Maintain separate execution domains for running processes	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 ↗

0819.09m1Organizational.23-09.m 09.06 Network Security Management

ID: 0819.09m1Organizational.23-09.m 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 ↗
Require interconnection security agreements ↗	CMA_C1151 - Require interconnection security agreements	Manual, Disabled	1.1.0 ↗

0821.09m2Organizational.2-09.m 09.06 Network Security Management

ID: 0821.09m2Organizational.2-09.m 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 ↗
Configure actions for noncompliant devices ↗	CMA_0062 - Configure actions for noncompliant devices	Manual, Disabled	1.1.0 ↗
Create configuration plan protection ↗	CMA_C1233 - Create configuration plan protection	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 ↗
Develop and maintain baseline configurations ↗	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	1.1.0 ↗
Develop configuration item identification plan ↗	CMA_C1231 - Develop configuration item identification plan	Manual, Disabled	1.1.0 ↗
Develop configuration management plan ↗	CMA_C1232 - Develop configuration management plan	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 a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	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 ↗
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 an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	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	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 ↗
Review changes for any unauthorized changes ↗	CMA_C1204 - Review changes for any unauthorized changes	Manual, Disabled	1.1.0 ↗

0822.09m2Organizational.4-09.m 09.06 Network Security Management

ID: 0822.09m2Organizational.4-09.m 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 ↗
Control information flow ↗	CMA_0079 - Control information flow	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 ↗
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 ↗
Route traffic through authenticated proxy network ↗	CMA_C1633 - Route traffic through authenticated proxy network	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 ↗

0824.09m3Organizational.1-09.m 09.06 Network Security Management

ID: 0824.09m3Organizational.1-09.m 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 ↗
Configure detection whitelist ↗	CMA_0068 - Configure detection whitelist	Manual, Disabled	1.1.0 ↗
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	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 ↗
Separately store backup information ↗	CMA_C1293 - Separately store backup information	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 ↗

0825.09m3Organizational.23-09.m 09.06 Network Security Management

ID: 0825.09m3Organizational.23-09.m 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 ↗
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 ↗
Document wireless access security controls ↗	CMA_C1695 - Document wireless access security controls	Manual, Disabled	1.1.0 ↗
Implement system boundary protection ↗	CMA_0328 - Implement system boundary protection	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 ↗
Provide monitoring information as needed ↗	CMA_C1689 - Provide monitoring information as needed	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 ↗

0826.09m3Organizational.45-09.m 09.06 Network Security Management

ID: 0826.09m3Organizational.45-09.m Ownership: Shared

Expand table

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 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	Manual, Disabled	1.1.0 ↗

0828.09m3Organizational.8-09.m 09.06 Network Security Management

ID: 0828.09m3Organizational.8-09.m 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 ↗

0829.09m3Organizational.911-09.m 09.06 Network Security Management

ID: 0829.09m3Organizational.911-09.m Ownership: Shared

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

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 ↗

0830.09m3Organizational.1012-09.m 09.06 Network Security Management

ID: 0830.09m3Organizational.1012-09.m 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, monitor, and control voip ↗	CMA_0025 - Authorize, monitor, and control voip	Manual, Disabled	1.1.0 ↗
Enforce user uniqueness ↗	CMA_0250 - Enforce user uniqueness	Manual, Disabled	1.1.0 ↗

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 ↗
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	1.1.0 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	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 ↗

0832.09m3Organizational.14-09.m 09.06 Network Security Management

ID: 0832.09m3Organizational.14-09.m 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 ↗
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 ↗

0835.09n1Organizational.1-09.n 09.06 Network Security Management

ID: 0835.09n1Organizational.1-09.n Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[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 ↴
Configure detection whitelist ↴	CMA_0068 - Configure detection whitelist	Manual, Disabled	1.1.0 ↴
Require interconnection security agreements ↴	CMA_C1151 - Require interconnection security agreements	Manual, Disabled	1.1.0 ↴
Secure the interface to external systems ↴	CMA_0491 - Secure the interface to external systems	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 ↴
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 ↴

0836.09.n2Organizational.1-09.n 09.06 Network Security Management

ID: 0836.09.n2Organizational.1-09.n Ownership: Shared

[] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[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 ↴
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 ↴
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 ↴

0837.09.n2Organizational.2-09.n 09.06 Network Security Management

ID: 0837.09.n2Organizational.2-09.n 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 ↴
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 ↴

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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 external providers consistently meet interests of the customers ↗	CMA_C1592 - Ensure external providers consistently meet interests of the customers	Manual, Disabled	1.1.0 ↗
Identify external service providers ↗	CMA_C1591 - Identify external service providers	Manual, Disabled	1.1.0 ↗
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 ↗
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 interconnection security agreements ↗	CMA_C1151 - Require interconnection security agreements	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 ↗

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

0850.01o1Organizational.12-01.o 01.04 Network Access Control

ID: 0850.01o1Organizational.12-01.o 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	1.1.0 ↗

0858.09m1Organizational.4-09.m 09.06 Network Security Management

ID: 0858.09m1Organizational.4-09.m Ownership: Shared

[\[\]](#) Expand table

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 ↗
Document and implement wireless access guidelines ↗	CMA_0190 - Document and implement wireless access guidelines	Manual, Disabled	1.1.0 ↗
Document wireless access security	CMA_C1695 - Document wireless access security controls	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
controls ↗			
Identify and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	1.1.0 ↗
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 ↗
Protect wireless access ↗	CMA_0411 - Protect wireless access	Manual, Disabled	1.1.0 ↗
Windows machines should meet requirements for 'Windows Firewall Properties' ↗	Windows machines should have the specified Group Policy settings in the category 'Windows Firewall Properties' for firewall state, connections, rule management, and notifications. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗

0859.09m1Organizational.78-09.m 09.06 Network Security Management

ID: 0859.09m1Organizational.78-09.m Ownership: Shared

[\[\]](#) 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	3.0.0 ↗
Control information flow ↗	CMA_0079 - Control information flow	Manual, Disabled	1.1.0 ↗

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 ↗
Employ flow control mechanisms of encrypted information ↗	CMA_0211 - Employ flow control mechanisms of encrypted information	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 ↗
Information flow control using security policy filters ↗	CMA_C1029 - Information flow control using security policy filters	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 ↗
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 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	Manual, Disabled	1.1.0 ↗
Separate duties of individuals ↗	CMA_0492 - Separate duties of individuals	Manual, Disabled	1.1.0 ↗

0860.09m1Organizational.9-09.m 09.06 Network Security Management

ID: 0860.09m1Organizational.9-09.m Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Deploy Diagnostic Settings for Network Security Groups ↗	This policy automatically deploys diagnostic settings to network security groups. A storage account with name '{storagePrefixParameter}{NSGLocation}' will be automatically created.	deployIfNotExists	2.0.1 ↗
Establish an alternate processing site ↗	CMA_0262 - Establish an alternate processing site	Manual, Disabled	1.1.0 ↗
Implement managed interface for each external service ↗	CMA_C1626 - Implement managed interface for each external service	Manual, Disabled	1.1.0 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	Manual, Disabled	1.1.0 ↗
Separately store backup information ↗	CMA_C1293 - Separately store backup information	Manual, Disabled	1.1.0 ↗

0861.09m2Organizational.67-09.m 09.06 Network Security Management

ID: 0861.09m2Organizational.67-09.m Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
App Service apps should use a virtual network service endpoint ↗	Use virtual network service endpoints to restrict access to your app from selected subnets from an Azure virtual network. To learn more about App Service service endpoints, visit https://aka.ms/appservice-vnet-service-endpoint ↗.	AuditIfNotExists, Disabled	2.0.1 ↗
Document and implement wireless access guidelines ↗	CMA_0190 - Document and implement wireless access guidelines	Manual, Disabled	1.1.0 ↗

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 ↗
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 ↗
Protect wireless access ↗	CMA_0411 - Protect wireless access	Manual, Disabled	1.1.0 ↗
Windows machines should meet requirements for 'Security Options - Network Access' ↗	Windows machines should have the specified Group Policy settings in the category 'Security Options - Network Access' for including access for anonymous users, local accounts, and remote access to the registry. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗ .	AuditIfNotExists, Disabled	3.0.0 ↗

0862.09m2Organizational.8-09.m 09.06 Network Security Management

ID: 0862.09m2Organizational.8-09.m 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	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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
SQL Server should use a virtual network service endpoint ↗	This policy audits any SQL Server not configured to use a virtual network service endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗

0863.09m2Organizational.910-09.m 09.06 Network Security Management

ID: 0863.09m2Organizational.910-09.m 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 ↗
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Configure actions for noncompliant devices ↗	CMA_0062 - Configure actions for noncompliant devices	Manual, Disabled	1.1.0 ↗
Develop a concept of operations (CONOPS) ↗	CMA_0141 - Develop a concept of operations (CONOPS)	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 and maintain a vulnerability management standard ↗	CMA_0152 - Develop and maintain a vulnerability management standard	Manual, Disabled	1.1.0 ↗
Develop and maintain baseline configurations ↗	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	1.1.0 ↗
Develop configuration item identification plan ↗	CMA_C1231 - Develop configuration item identification plan	Manual, Disabled	1.1.0 ↗
Develop information security policies and procedures ↗	CMA_0158 - Develop information security policies	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	and procedures		
Develop SSP that meets criteria ↗	CMA_C1492 - Develop SSP that meets criteria	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 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 and document a configuration management plan ↗	CMA_0264 - Establish and document a configuration management 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 connected devices ↗	CMA_0279 - Establish security requirements for the manufacturing of connected devices	Manual, Disabled	1.1.0 ↗
Event Hub should use a virtual network service endpoint ↗	This policy audits any Event Hub not configured to use a virtual network service endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗
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 ↗
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Review and update the information security architecture ↗	CMA_C1504 - Review and update the information security architecture	Manual, Disabled	1.1.0 ↗

0864.09m2Organizational.12-09.m 09.06 Network Security Management

ID: 0864.09m2Organizational.12-09.m 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 ↗
Cosmos DB should use a virtual network service endpoint ↗	This policy audits any Cosmos DB not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0 ↗
Establish voip usage restrictions ↗	CMA_0280 - Establish voip usage restrictions	Manual, Disabled	1.1.0 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	Manual, Disabled	1.1.0 ↗

0865.09m2Organizational.13-09.m 09.06 Network Security Management

ID: 0865.09m2Organizational.13-09.m 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 ↗
Employ restrictions on external system interconnections ↗	CMA_C1155 - Employ restrictions on external system interconnections	Manual, Disabled	1.1.0 ↗
Key Vault should use a virtual network service endpoint ↗	This policy audits any Key Vault not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0 ↗
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 ↗

0866.09m3Organizational.1516-09.m 09.06 Network Security Management

ID: 0866.09m3Organizational.1516-09.m 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 ↗
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 ↗

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 ↗
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	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 ↗
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	1.1.0 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	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 ↗

0868.09m3Organizational.18-09.m 09.06 Network Security Management

ID: 0868.09m3Organizational.18-09.m Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Container Registry should use a virtual network service endpoint ↗	This policy audits any Container Registry not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0- preview ↗

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 managed interface for each external service 🔗	CMA_C1626 - Implement managed interface for each external service	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 🔗
Secure the interface to external systems 🔗	CMA_0491 - Secure the interface to external systems	Manual, Disabled	1.1.0 🔗

0869.09m3Organizational.19-09.m 09.06 Network Security Management

ID: 0869.09m3Organizational.19-09.m Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Container Registry should use a virtual network service endpoint 🔗	This policy audits any Container Registry not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0-preview 🔗
Configure actions for noncompliant devices 🔗	CMA_0062 - Configure actions for noncompliant devices	Manual, Disabled	1.1.0 🔗
Create configuration plan protection 🔗	CMA_C1233 - Create configuration plan protection	Manual, Disabled	1.1.0 🔗
Develop and maintain baseline configurations 🔗	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	1.1.0 🔗
Develop configuration item identification plan 🔗	CMA_C1231 - Develop configuration item identification plan	Manual, Disabled	1.1.0 🔗
Develop configuration management plan 🔗	CMA_C1232 - Develop configuration management plan	Manual, Disabled	1.1.0 🔗
Employ automatic shutdown/restart when	CMA_C1715 - Employ automatic shutdown/restart when violations	Manual, Disabled	1.1.0 🔗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
violations are detected ↗	are detected		
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 ↗

0870.09m3Organizational.20-09.m 09.06 Network Security Management

ID: 0870.09m3Organizational.20-09.m Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Container Registry should use a virtual network service endpoint ↗	This policy audits any Container Registry not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0-preview ↗
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 ↗
Enforce user uniqueness ↗	CMA_0250 - Enforce user uniqueness	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 external service providers ↗	CMA_C1591 - Identify external service providers	Manual, Disabled	1.1.0 ↗
Implement managed interface for each external service ↗	CMA_C1626 - Implement managed interface for each external service	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Route traffic through authenticated proxy network ↗	CMA_C1633 - Route traffic through authenticated proxy network	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 ↗

0871.09m3Organizational.22-09.m 09.06 Network Security Management

ID: 0871.09m3Organizational.22-09.m Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Container Registry should use a virtual network service endpoint ↗	This policy audits any Container Registry not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0-preview ↗
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 ↗
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↗

0885.09n2Organizational.3-09.n 09.06 Network Security Management

ID: 0885.09n2Organizational.3-09.n Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Network traffic data collection agent should be	Security Center uses the Microsoft Dependency agent to collect network traffic data from your Azure virtual	AuditIfNotExists, Disabled	1.0.2-preview ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
installed on Linux virtual machines ↗	machines to enable advanced network protection features such as traffic visualization on the network map, network hardening recommendations and specific network threats.		
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 ↗

0886.09n2Organizational.4-09.n 09.06 Network Security Management

ID: 0886.09n2Organizational.4-09.n 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 ↗
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 ↗

0887.09n2Organizational.5-09.n 09.06 Network Security Management

ID: 0887.09n2Organizational.5-09.n Ownership: Shared

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[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 ↗
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 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	Manual, Disabled	1.1.0 ↗

0888.09n2Organizational.6-09.n 09.06 Network Security Management

ID: 0888.09n2Organizational.6-09.n 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 ↗
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 ↗

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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 external providers consistently meet interests of the customers ↗	CMA_C1592 - Ensure external providers consistently meet interests of the customers	Manual, Disabled	1.1.0 ↗
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 ↗
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 ↗

0894.01m2Organizational.7-01.m 01.04 Network Access Control

ID: 0894.01m2Organizational.7-01.m Ownership: Shared

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
[Preview]: Container Registry should use a virtual network service endpoint ↗	This policy audits any Container Registry not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0-preview ↗
App Service apps should use a virtual network service endpoint ↗	Use virtual network service endpoints to restrict access to your app from selected subnets from an Azure virtual network. To learn more about App Service service endpoints, visit https://aka.ms/appservice-vnet-service-endpoint ↗.	AuditIfNotExists, Disabled	2.0.1 ↗
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 ↗
Cosmos DB should use a virtual network service endpoint ↗	This policy audits any Cosmos DB not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0 ↗
Deploy network watcher when virtual networks are created ↗	This policy creates a network watcher resource in regions with virtual networks. You need to ensure existence of a resource group named networkWatcherRG, which will be used to deploy network watcher instances.	DeployIfNotExists	1.0.0 ↗
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 ↗
Event Hub should use a virtual network service endpoint ↗	This policy audits any Event Hub not configured to use a virtual network service endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Gateway subnets should not be configured with a network security group ↗	This policy denies if a gateway subnet is configured with a network security group. Assigning a network security group to a gateway subnet will cause the gateway to stop functioning.	deny	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 https://aka.ms/nsgr-doc ↗	AuditIfNotExists, Disabled	3.0.0 ↗
Key Vault should use a virtual network service endpoint ↗	This policy audits any Key Vault not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0 ↗
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 ↗
Route traffic through authenticated proxy network ↗	CMA_C1633 - Route traffic through authenticated proxy network	Manual, Disabled	1.1.0 ↗
SQL Server should use a virtual network service endpoint ↗	This policy audits any SQL Server not configured to use a virtual network service endpoint.	AuditIfNotExists, Disabled	1.0.0 ↗
Storage Accounts should use a virtual network service endpoint ↗	This policy audits any Storage Account not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0 ↗
Subnets should be associated with a Network Security Group ↗	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)	AuditIfNotExists, Disabled	3.0.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
rules that allow or deny network traffic to your subnet.			
Virtual machines should be connected to an approved virtual network ↗	This policy audits any virtual machine connected to a virtual network that is not approved.	Audit, Deny, Disabled	1.0.0 ↗

Back-up

Workforce members roles and responsibilities in the data backup process are identified and communicated to the workforce; in particular, Bring Your Own Device (BYOD) users are required to perform backups of organizational and/or client data on their devices.

ID: 1699.09I1Organizational.10 - 09.I Ownership: Customer

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

Name	Description	Effect(s)	Version
(Azure portal)		(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 ↗

Network Controls

Wireless access points are placed in secure areas and shut down when not in use (e.g. nights, weekends).

ID: 0867.09m3Organizational.17 - 09.m Ownership: Customer

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

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Storage Accounts should use a virtual network service endpoint ↴	This policy audits any Storage Account not configured to use a virtual network service endpoint.	Audit, Disabled	1.0.0 ↴

On-line Transactions

The organization requires the use of encryption between, and the use of electronic signatures by, each of the parties involved in the transaction.

ID: 0946.09y2Organizational.14 - 09.y Ownership: Customer

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

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

09 Transmission Protection

0901.09s1Organizational.1-09.s 09.08 Exchange of Information

ID: 0901.09s1Organizational.1-09.s Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
App Service apps should not have CORS configured to	Cross-Origin Resource Sharing (CORS) should not allow all domains to access your app. Allow	AuditIfNotExists, Disabled	2.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
allow every resource to access your apps ↗	only required domains to interact with your app.		
Categorize information ↗	CMA_0052 - Categorize information	Manual, Disabled	1.1.0 ↗
Configure actions for noncompliant devices ↗	CMA_0062 - Configure actions for noncompliant devices	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 ↗
Develop acceptable use policies and procedures ↗	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	1.1.0 ↗
Develop and maintain baseline configurations ↗	CMA_0153 - Develop and maintain baseline configurations	Manual, Disabled	1.1.0 ↗
Develop business classification schemes ↗	CMA_0155 - Develop business classification schemes	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 personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	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 ↗
Enforce security configuration settings ↗	CMA_0249 - Enforce security configuration settings	Manual, Disabled	1.1.0 ↗
Ensure security categorization is approved ↗	CMA_C1540 - Ensure security categorization is approved	Manual, Disabled	1.1.0 ↗
Establish a configuration control board ↗	CMA_0254 - Establish a configuration control board	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 a configuration management plan ↗	CMA_0264 - Establish and document a configuration management plan	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish terms and conditions for processing resources ↗	CMA_C1077 - Establish terms and conditions for processing resources	Manual, Disabled	1.1.0 ↗
Implement an automated configuration management tool ↗	CMA_0311 - Implement an automated configuration management tool	Manual, Disabled	1.1.0 ↗
Implement controls to secure all media ↗	CMA_0314 - Implement controls to secure all media	Manual, Disabled	1.1.0 ↗
Perform information input validation ↗	CMA_C1723 - Perform information input validation	Manual, Disabled	1.1.0 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	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 ↗
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Review label activity and analytics ↗	CMA_0474 - Review label activity and analytics	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 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3	CMA_0522 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
years ↗	every 3 years		

0902.09s2Organizational.13-09.s 09.08 Exchange of Information

ID: 0902.09s2Organizational.13-09.s 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 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 ↗
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 ↗
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 ↗
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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Protect data in transit using encryption ↗	CMA_0403 - Protect data in transit using encryption	Manual, Disabled	1.1.0 ↗
Provide capability to disconnect or disable remote access ↗	CMA_C1066 - Provide capability to disconnect or disable remote access	Manual, Disabled	1.1.0 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	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 ↗

0903.10f1Organizational.1-10.f 10.03 Cryptographic Controls

ID: 0903.10f1Organizational.1-10.f 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	1.1.0 ↗
Define cryptographic use ↗	CMA_0120 - Define cryptographic use	Manual, Disabled	1.1.0 ↗
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	1.1.0 ↗

0904.10f2Organizational.1-10.f 10.03 Cryptographic Controls

ID: 0904.10f2Organizational.1-10.f 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 a physical key management process ↗	CMA_0115 - Define a physical key management process	Manual, Disabled	1.1.0 ↗
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 ↗
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 ↗
Produce, control and distribute symmetric cryptographic keys ↗	CMA_C1645 - Produce, control and distribute 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 ↗

0912.09s1Organizational.4-09.s 09.08 Exchange of Information

ID: 0912.09s1Organizational.4-09.s Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
App Service apps should have remote debugging turned off ↗	Remote debugging requires inbound ports to be opened on an App	AuditIfNotExists, Disabled	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Service app. Remote debugging should be turned off.		
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 ↗
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 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	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 ↗

0913.09s1Organizational.5-09.s 09.08 Exchange of Information

ID: 0913.09s1Organizational.5-09.s 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	1.1.0 ↗
Define cryptographic use ↗	CMA_0120 - Define cryptographic use	Manual, Disabled	1.1.0 ↗
Function apps should have remote debugging turned off ↗	Remote debugging requires inbound ports to be opened on Function apps.	AuditIfNotExists, Disabled	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	Remote debugging should be turned off.		
Produce, control and distribute asymmetric cryptographic keys ↗	CMA_C1646 - Produce, control and distribute asymmetric cryptographic keys	Manual, Disabled	1.1.0 ↗
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	1.1.0 ↗

0914.09s1Organizational.6-09.s 09.08 Exchange of Information

ID: 0914.09s1Organizational.6-09.s 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 ↗
Employ independent assessors to conduct security control assessments ↗	CMA_C1148 - Employ independent assessors to conduct security control assessments	Manual, Disabled	1.1.0 ↗
Produce Security Assessment report ↗	CMA_C1146 - Produce Security Assessment report	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 ↗

0915.09s2Organizational.2-09.s 09.08 Exchange of Information

ID: 0915.09s2Organizational.2-09.s Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
App Service apps should have Client Certificates (Incoming client certificates) enabled ↗	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	1.0.0 ↗
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	Manual, Disabled	1.1.0 ↗
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 ↗

0916.09s2Organizational.4-09.s 09.08 Exchange of Information

ID: 0916.09s2Organizational.4-09.s 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 ↗
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 ↗
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	Manual, Disabled	1.1.0 ↗
Explicitly notify use of collaborative computing devices ↗	CMA_C1649 - Explicitly notify use of collaborative computing devices	Manual, Disabled	1.1.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Identify and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	1.1.0 ↗
Prohibit remote activation of collaborative computing devices ↗	CMA_C1648 - Prohibit remote activation of collaborative computing devices	Manual, Disabled	1.1.0 ↗
Restrict media use ↗	CMA_0450 - Restrict media use	Manual, Disabled	1.1.0 ↗

0926.09v1Organizational.2-09.v 09.08 Exchange of Information

ID: 0926.09v1Organizational.2-09.v 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	1.1.0 ↗
Implement a fault tolerant name/address service ↗	CMA_0305 - Implement a fault tolerant name/address service	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 passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	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 ↗

0927.09v1Organizational.3-09.v 09.08 Exchange of Information

ID: 0927.09v1Organizational.3-09.v 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 ↗
Enforce user uniqueness ↗	CMA_0250 - Enforce user uniqueness	Manual, Disabled	1.1.0 ↗
Identify and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	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 ↗

0928.09v1Organizational.45-09.v 09.08 Exchange of Information

ID: 0928.09v1Organizational.45-09.v 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	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 ↗
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 ↗
Produce, control and distribute asymmetric cryptographic keys ↗	CMA_C1646 - Produce, control and distribute asymmetric cryptographic keys	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	1.1.0 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	Manual, Disabled	1.1.0 ↗

0929.09v1Organizational.6-09.v 09.08 Exchange of Information

ID: 0929.09v1Organizational.6-09.v 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	1.1.0 ↗
Control information flow ↗	CMA_0079 - Control information flow	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 ↗
Produce, control and distribute asymmetric cryptographic keys ↗	CMA_C1646 - Produce, control and distribute asymmetric cryptographic keys	Manual, Disabled	1.1.0 ↗
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	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 ↗

0943.09y1Organizational.1-09.y 09.09 Electronic Commerce Services

ID: 0943.09y1Organizational.1-09.y 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	1.1.0 ↗
Document process to ensure integrity of PII ↗	CMA_C1827 - Document process to ensure integrity of PII	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 ↗

0944.09y1Organizational.2-09.y 09.09 Electronic Commerce Services

ID: 0944.09y1Organizational.2-09.y 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	1.1.0 ↗
Control information flow ↗	CMA_0079 - Control information	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	flow	Disabled	
Employ boundary protection to isolate information systems 🔗	CMA_C1639 - Employ boundary protection to isolate information systems	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 
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 
Information flow control using security policy filters 🔗	CMA_C1029 - Information flow control using security policy filters	Manual, Disabled	1.1.0 

0945.09y1Organizational.3-09.y 09.09 Electronic Commerce Services

ID: 0945.09y1Organizational.3-09.y Ownership: Shared

 [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit Windows machines that do not contain the specified certificates in Trusted Root 🔗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol  . Machines are non-compliant if the machine Trusted Root certificate store (Cert:\LocalMachine\Root) does not contain one or more of the certificates listed by the policy parameter.	auditIfNotExists	3.0.0 
Authenticate to cryptographic module 🔗	CMA_0021 - Authenticate to cryptographic module	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 ↗
Define cryptographic use ↗	CMA_0120 - Define cryptographic use	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 passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	1.1.0 ↗

0947.09y2Organizational.2-09.y 09.09 Electronic Commerce Services

ID: 0947.09y2Organizational.2-09.y 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 ↗
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	Manual, Disabled	1.1.0 ↗
Enforce SSL connection should be enabled for PostgreSQL database servers ↗	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	1.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Establish a data leakage management procedure ↗	CMA_0255 - Establish a data leakage management procedure	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 ↗
Govern and monitor audit processing activities ↗	CMA_0289 - Govern and monitor audit processing activities	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗
Protect special information ↗	CMA_0409 - Protect special information	Manual, Disabled	1.1.0 ↗
Restrict location of information processing, storage and services ↗	CMA_C1593 - Restrict location of information processing, storage and services	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 ↗

0948.09y2Organizational.3-09.y 09.09 Electronic Commerce Services

ID: 0948.09y2Organizational.3-09.y 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	1.1.0 ↗
Distribute authenticators ↗	CMA_0184 - Distribute authenticators	Manual, Disabled	1.1.0 ↗
Enforce random unique session identifiers ↗	CMA_0247 - Enforce random unique session identifiers	Manual, Disabled	1.1.0 ↗
Enforce SSL connection should be enabled for MySQL database servers ↗	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	1.0.1 ↗
Issue public key certificates ↗	CMA_0347 - Issue public key certificates	Manual, Disabled	1.1.0 ↗
Satisfy token quality requirements ↗	CMA_0487 - Satisfy token quality requirements	Manual, Disabled	1.1.0 ↗

0949.09y2Organizational.5-09.y 09.09 Electronic Commerce Services

ID: 0949.09y2Organizational.5-09.y 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 use the	Periodically, newer versions are released for TLS either due to security flaws, include	AuditIfNotExists, Disabled	2.0.1 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
latest TLS version ↗	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.		
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 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 ↗
Identify external service providers ↗	CMA_C1591 - Identify external service providers	Manual, Disabled	1.1.0 ↗
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 ↗

0960.09sCSPOrganizational.1-09.s 09.08 Exchange of Information

ID: 0960.09sCSPOrganizational.1-09.s **Ownership:** Shared

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Identify external service providers ↗	CMA_C1591 - Identify external service providers	Manual, Disabled	1.1.0 ↗

099.09m2Organizational.11-09.m 09.06 Network Security Management

ID: 099.09m2Organizational.11-09.m 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	1.1.0 ↗
Define cryptographic use ↗	CMA_0120 - Define cryptographic use	Manual, Disabled	1.1.0 ↗
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	1.1.0 ↗

Control of Operational Software

Applications and operating systems are successfully tested for usability, security and impact prior to production.

ID: 0606.10h2System.1 - 10.h Ownership: Customer

[\[\]](#) Expand table

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

The organization uses its configuration control program to maintain control of all implemented software and its system documentation and archive prior versions of

implemented software and associated system documentation.

ID: 0607.10h2System.23 - 10.h Ownership: Customer

[] 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 ↗
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	3.0.0 ↗

10 Password Management

1002.01d1System.1-01.d 01.02 Authorized Access to Information Systems

ID: 1002.01d1System.1-01.d 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	1.1.0 ↗

1003.01d1System.3-01.d 01.02 Authorized Access to Information Systems

ID: 1003.01d1System.3-01.d Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement training for protecting authenticators ↗	CMA_0329 - Implement training for protecting authenticators	Manual, Disabled	1.1.0 ↗
Refresh authenticators ↗	CMA_0425 - Refresh authenticators	Manual, Disabled	1.1.0 ↗
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	1.1.0 ↗

1004.01d1System.8913-01.d 01.02 Authorized Access to Information Systems

ID: 1004.01d1System.8913-01.d 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	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)
Manage authenticator lifetime and reuse ↗	CMA_0355 - Manage authenticator lifetime and reuse	Manual, Disabled	1.1.0 ↗
Manage Authenticators ↗	CMA_C1321 - Manage Authenticators	Manual, Disabled	1.1.0 ↗
Protect passwords with encryption ↗	CMA_0408 - Protect passwords with encryption	Manual, Disabled	1.1.0 ↗
Refresh authenticators ↗	CMA_0425 - Refresh authenticators	Manual, Disabled	1.1.0 ↗
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	1.1.0 ↗

1005.01d1System.1011-01.d 01.02 Authorized Access to Information Systems

ID: 1005.01d1System.1011-01.d 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 ↗
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 ↗
Produce, control and distribute symmetric cryptographic keys ↗	CMA_C1645 - Produce, control and distribute symmetric cryptographic keys	Manual, Disabled	1.1.0 ↗

1006.01d2System.1-01.d 01.02 Authorized Access to Information Systems

ID: 1006.01d2System.1-01.d 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 ↗
Generate error messages ↗	CMA_C1724 - Generate error messages	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 training for protecting authenticators ↗	CMA_0329 - Implement training for protecting authenticators	Manual, Disabled	1.1.0 ↗
Obscure feedback information during authentication process ↗	CMA_C1344 - Obscure feedback information during authentication process	Manual, Disabled	1.1.0 ↗

1007.01d2System.2-01.d 01.02 Authorized Access to Information Systems

ID: 1007.01d2System.2-01.d Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define cryptographic use ↗	CMA_0120 - Define cryptographic use	Manual, Disabled	1.1.0 ↗

1008.01d2System.3-01.d 01.02 Authorized Access to Information Systems

ID: 1008.01d2System.3-01.d 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 ↗
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	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 ↗
Enforce rules of behavior and access agreements ↗	CMA_0248 - Enforce rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Establish a data leakage management procedure ↗	CMA_0255 - Establish a data leakage management procedure	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 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0 ↗
Protect special information ↗	CMA_0409 - Protect special information	Manual, Disabled	1.1.0 ↗
Require users to sign access agreement ↗	CMA_0440 - Require users to sign access agreement	Manual, Disabled	1.1.0 ↗
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗
Update organizational access agreements ↗	CMA_0520 - Update organizational access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0 ↗

1009.01d2System.4-01.d 01.02 Authorized Access to Information Systems

ID: 1009.01d2System.4-01.d 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	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 ↗
Refresh authenticators ↗	CMA_0425 - Refresh authenticators	Manual, Disabled	1.1.0 ↗

1014.01d1System.12-01.d 01.02 Authorized Access to Information Systems

ID: 1014.01d1System.12-01.d 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	1.1.0 ↗
Establish a password policy ↗	CMA_0256 - Establish a password policy	Manual, Disabled	1.1.0 ↗
Establish authenticator types and processes ↗	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	1.1.0 ↗
Establish procedures for initial authenticator distribution ↗	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement parameters for memorized secret verifiers ↗	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	1.1.0 ↗
Implement training for protecting authenticators ↗	CMA_0329 - Implement training for protecting authenticators	Manual, Disabled	1.1.0 ↗
Manage authenticator lifetime and reuse ↗	CMA_0355 - Manage authenticator lifetime and reuse	Manual, Disabled	1.1.0 ↗
Manage Authenticators ↗	CMA_C1321 - Manage Authenticators	Manual, Disabled	1.1.0 ↗
Refresh authenticators ↗	CMA_0425 - Refresh authenticators	Manual, Disabled	1.1.0 ↗
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 ↗

1015.01d1System.14-01.d 01.02 Authorized Access to Information Systems

ID: 1015.01d1System.14-01.d Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish authenticator types and processes ↗	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	1.1.0 ↗
Establish procedures for initial authenticator distribution ↗	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	1.1.0 ↗
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 ↗

1022.01d1System.15-01.d 01.02 Authorized Access to Information Systems

ID: 1022.01d1System.15-01.d 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 ↗
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	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 and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	1.1.0 ↗
Implement parameters for memorized secret verifiers ↗	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	1.1.0 ↗
Refresh authenticators ↗	CMA_0425 - Refresh authenticators	Manual, Disabled	1.1.0 ↗
Restrict media use ↗	CMA_0450 - Restrict media use	Manual, Disabled	1.1.0 ↗

1031.01d1System.34510-01.d 01.02 Authorized Access to Information Systems

ID: 1031.01d1System.34510-01.d Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document security strength requirements in acquisition	CMA_0203 - Document security strength requirements in acquisition	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
contracts ↗	contracts		
Establish a password policy ↗	CMA_0256 - Establish a password policy	Manual, Disabled	1.1.0 ↗
Establish procedures for initial authenticator distribution ↗	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	1.1.0 ↗
Implement parameters for memorized secret verifiers ↗	CMA_0321 - Implement parameters for memorized secret verifiers	Manual, Disabled	1.1.0 ↗
Manage Authenticators ↗	CMA_C1321 - Manage Authenticators	Manual, Disabled	1.1.0 ↗
Refresh authenticators ↗	CMA_0425 - Refresh authenticators	Manual, Disabled	1.1.0 ↗

11 Access Control

1106.01b1System.1-01.b 01.02 Authorized Access to Information Systems

ID: 1106.01b1System.1-01.b Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign account managers ↗	CMA_0015 - Assign account managers	Manual, Disabled	1.1.0 ↗
Audit user account status ↗	CMA_0020 - Audit user account status	Manual, Disabled	1.1.0 ↗
Define information system account types ↗	CMA_0121 - Define information system account types	Manual, Disabled	1.1.0 ↗
Document access privileges ↗	CMA_0186 - Document access privileges	Manual, Disabled	1.1.0 ↗
Establish conditions for role membership ↗	CMA_0269 - Establish conditions for role membership	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 user accounts ↗	CMA_0480 - Review user accounts	Manual, Disabled	1.1.0 ↗
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	1.1.0 ↗

1107.01b1System.2-01.b 01.02 Authorized Access to Information Systems

ID: 1107.01b1System.2-01.b Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish authenticator types and processes ↗	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	1.1.0 ↗
Establish procedures for initial authenticator distribution ↗	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	1.1.0 ↗
Manage Authenticators ↗	CMA_C1321 - Manage Authenticators	Manual, Disabled	1.1.0 ↗
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	1.1.0 ↗

1108.01b1System.3-01.b 01.02 Authorized Access to Information Systems

ID: 1108.01b1System.3-01.b Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign account managers ↗	CMA_0015 - Assign account managers	Manual, Disabled	1.1.0 ↗
Define information system account types ↗	CMA_0121 - Define information system account types	Manual, Disabled	1.1.0 ↗
Monitor account activity ↗	CMA_0377 - Monitor account activity	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 ↗

1109.01b1System.479-01.b 01.02 Authorized Access to Information Systems

ID: 1109.01b1System.479-01.b 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 ↗
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 ↗
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	1.1.0 ↗
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	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 ↗
Initiate transfer or reassignment actions ↗	CMA_0333 - Initiate transfer or reassignment actions	Manual, Disabled	1.1.0 ↗
Manage Authenticators ↗	CMA_C1321 - Manage Authenticators	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Modify access authorizations upon personnel transfer ↗	CMA_0374 - Modify access authorizations upon personnel transfer	Manual, Disabled	1.1.0 ↗
Notify upon termination or transfer ↗	CMA_0381 - Notify upon termination or transfer	Manual, Disabled	1.1.0 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	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 ↗
Provide periodic security awareness training ↗	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 ↗
Provide security awareness training for insider threats ↗	CMA_0417 - Provide security awareness training for insider threats	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 ↗
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 ↗
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	1.1.0 ↗
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	1.1.0 ↗

1110.01b1System.5-01.b 01.02 Authorized Access to Information Systems

ID: 1110.01b1System.5-01.b 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 ↗
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 personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	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 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0 ↗
Reissue authenticators for changed groups and accounts ↗	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	1.1.0 ↗
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗

Name	Description	Effect(s)	Version
(GitHub)		(GitHub)	
		every 3 years	

11109.01q1Organizational.57-01.q 01.05 Operating System Access Control

ID: 11109.01q1Organizational.57-01.q Ownership: Shared

[\[\]](#) Expand table

Name	Description	Effect(s)	Version
(GitHub)		(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 ↗
Adopt biometric authentication mechanisms ↗	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	1.1.0 ↗
Assign system identifiers ↗	CMA_0018 - Assign system identifiers	Manual, Disabled	1.1.0 ↗
Enforce user uniqueness ↗	CMA_0250 - Enforce user uniqueness	Manual, Disabled	1.1.0 ↗
Identify status of individual users ↗	CMA_C1316 - Identify status of individual users	Manual, Disabled	1.1.0 ↗
Prevent identifier reuse for the defined time period ↗	CMA_C1314 - Prevent identifier reuse for the defined time period	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 ↗

1111.01b2System.1-01.b 01.02 Authorized Access to Information Systems

ID: 1111.01b2System.1-01.b 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 ↗
Reissue authenticators for changed groups and accounts 🔗	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	1.1.0 ↗

1111.01q2System.4-01.q 01.05 Operating System Access Control

ID: 11111.01q2System.4-01.q Ownership: Shared

[Expand table](#)

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 ↗
Establish authenticator types and processes 🔗	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	1.1.0 ↗
Establish procedures for initial authenticator distribution 🔗	CMA_0276 - Establish procedures for initial authenticator distribution	Manual, Disabled	1.1.0 ↗
Verify identity before distributing authenticators 🔗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	1.1.0 ↗

1112.01q2Organizational.67-01.q 01.05 Operating System Access Control

ID: 11112.01q2Organizational.67-01.q 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 ↗
Adopt biometric authentication mechanisms ↗	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	1.1.0 ↗
Satisfy token quality requirements ↗	CMA_0487 - Satisfy token quality requirements	Manual, Disabled	1.1.0 ↗

1112.01b2System.2-01.b 01.02 Authorized Access to Information Systems

ID: 1112.01b2System.2-01.b 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 ↗
Distribute authenticators ↗	CMA_0184 - Distribute authenticators	Manual, Disabled	1.1.0 ↗
Ensure resources are authorized ↗	CMA_C1159 - Ensure resources are authorized	Manual, Disabled	1.1.0 ↗
Establish authenticator types and processes ↗	CMA_0267 - Establish authenticator types and processes	Manual, Disabled	1.1.0 ↗
Satisfy token quality requirements ↗	CMA_0487 - Satisfy token quality requirements	Manual, Disabled	1.1.0 ↗
Update the security authorization ↗	CMA_C1160 - Update the security authorization	Manual, Disabled	1.1.0 ↗
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	1.1.0 ↗

11126.01t1Organizational.12-01.t 01.05 Operating System Access Control

ID: 11126.01t1Organizational.12-01.t 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 ↗

1114.01h1Organizational.123-01.h 01.03 User Responsibilities

ID: 1114.01h1Organizational.123-01.h 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 ↗
Terminate user session automatically ↗	CMA_C1054 - Terminate user session automatically	Manual, Disabled	1.1.0 ↗

11154.02i1Organizational.5-02.i 02.04 Termination or Change of Employment

ID: 11154.02i1Organizational.5-02.i 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Initiate transfer or reassignment actions ↗	CMA_0333 - Initiate transfer or reassignment actions	Manual, Disabled	1.1.0 ↗
Modify access authorizations upon personnel transfer ↗	CMA_0374 - Modify access authorizations upon personnel transfer	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 ↗
Reevaluate access upon personnel transfer ↗	CMA_0424 - Reevaluate access upon personnel transfer	Manual, Disabled	1.1.0 ↗
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	1.1.0 ↗

11155.02i2Organizational.2-02.i 02.04 Termination or Change of Employment

ID: 11155.02i2Organizational.2-02.i Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate account management ↗	CMA_0026 - Automate account management	Manual, Disabled	1.1.0 ↗
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 ↗
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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Notify when account is not needed ↴	CMA_0383 - Notify when account is not needed	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 ↗
Retain terminated user data ↴	CMA_0455 - Retain terminated user data	Manual, Disabled	1.1.0 ↗

1116.01j1Organizational.145-01.j 01.04 Network Access Control

ID: 1116.01j1Organizational.145-01.j 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 ↗
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 ↗
Establish authenticator types and processes ↴	CMA_0267 - Establish authenticator types and processes	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)
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	1.1.0 ↗

1118.01j2Organizational.124-01.j 01.04 Network Access Control

ID: 1118.01j2Organizational.124-01.j Ownership: Shared

[\[\]](#) Expand table

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 ↗
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 ↗
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 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	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 ↗

11180.01c3System.6-01.c 01.02 Authorized Access to Information Systems

ID: 11180.01c3System.6-01.c 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 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege 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 ↗
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 ↗
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	1.1.0 ↗

1119.01j2Organizational.3-01.j 01.04 Network Access Control

ID: 1119.01j2Organizational.3-01.j Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enable detection of network devices ↗	CMA_0220 - Enable detection of network devices	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	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 ↗
Require interconnection security agreements ↗	CMA_C1151 - Require interconnection security agreements	Manual, Disabled	1.1.0 ↗
Secure the interface to external systems ↗	CMA_0491 - Secure the interface to external systems	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 ↗

11190.01t1Organizational.3-01.t 01.05 Operating System Access Control

ID: 11190.01t1Organizational.3-01.t 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 ↗
Control physical access ↗	CMA_0081 - Control physical access	Manual, Disabled	1.1.0 ↗
Identify and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	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 ↗
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 ↗

1120.09ab3System.9-09.ab 09.10 Monitoring

ID: 1120.09ab3System.9-09.ab Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Monitor should collect activity logs from all regions ↗	This policy audits the Azure Monitor log profile which does not export activities from all Azure supported regions including global.	AuditIfNotExists, Disabled	2.0.0 ↗

1121.01j3Organizational.2-01.j 01.04 Network Access Control

ID: 1121.01j3Organizational.2-01.j 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 ↗
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 ↗
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 user uniqueness ↗	CMA_0250 - Enforce user uniqueness	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 ↴
Notify users of system logon or access ↴	CMA_0382 - Notify users of system logon or access	Manual, Disabled	1.1.0 ↴
Provide privacy training ↴	CMA_0415 - Provide privacy training	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 ↴

11219.01b1Organizational.10-01.b 01.02 Authorized Access to Information Systems

ID: 11219.01b1Organizational.10-01.b 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 ↴
Design an access control model ↴	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↴
Document separation of duties ↴	CMA_0204 - Document separation of duties	Manual, Disabled	1.1.0 ↴
Employ least privilege access ↴	CMA_0212 - Employ least privilege access	Manual, Disabled	1.1.0 ↴
Separate duties of individuals ↴	CMA_0492 - Separate duties of individuals	Manual, Disabled	1.1.0 ↴

1122.01q1System.1-01.q 01.05 Operating System Access Control

ID: 1122.01q1System.1-01.q Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Accept only FICAM-approved third-party credentials ↗	CMA_C1348 - Accept only FICAM-approved third-party credentials	Manual, Disabled	1.1.0 ↗
Adopt biometric authentication mechanisms ↗	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	1.1.0 ↗
Conform to FICAM-issued profiles ↗	CMA_C1350 - Conform to FICAM-issued profiles	Manual, Disabled	1.1.0 ↗
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 ↗
Enforce user uniqueness ↗	CMA_0250 - Enforce user uniqueness	Manual, Disabled	1.1.0 ↗
Identify and authenticate non-organizational users ↗	CMA_C1346 - Identify and authenticate non-organizational users	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 ↗

11220.01b1System.10-01.b 01.02 Authorized Access to Information Systems

ID: 11220.01b1System.10-01.b Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign account managers ↗	CMA_0015 - Assign account managers	Manual, Disabled	1.1.0 ↗
Audit user account status ↗	CMA_0020 - Audit user account status	Manual, Disabled	1.1.0 ↗
Conduct exit interview upon termination ↗	CMA_0058 - Conduct exit interview upon termination	Manual, Disabled	1.1.0 ↗

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 ↗
Define information system account types ↗	CMA_0121 - Define information system account types	Manual, Disabled	1.1.0 ↗
Disable authenticators upon termination ↗	CMA_0169 - Disable authenticators upon termination	Manual, Disabled	1.1.0 ↗
Document access privileges ↗	CMA_0186 - Document access privileges	Manual, Disabled	1.1.0 ↗
Establish conditions for role membership ↗	CMA_0269 - Establish conditions for role membership	Manual, Disabled	1.1.0 ↗
Initiate transfer or reassignment actions ↗	CMA_0333 - Initiate transfer or reassignment actions	Manual, Disabled	1.1.0 ↗
Manage Authenticators ↗	CMA_C1321 - Manage Authenticators	Manual, Disabled	1.1.0 ↗
Modify access authorizations upon personnel transfer ↗	CMA_0374 - Modify access authorizations upon personnel transfer	Manual, Disabled	1.1.0 ↗
Monitor account activity ↗	CMA_0377 - Monitor account activity	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 ↗
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 ↗
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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Reevaluate access upon personnel transfer ↗	CMA_0424 - Reevaluate access upon personnel transfer	Manual, Disabled	1.1.0 ↗
Reissue authenticators for changed groups and accounts ↗	CMA_0426 - Reissue authenticators for changed groups and accounts	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 ↗
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 user accounts ↗	CMA_0480 - Review user accounts	Manual, Disabled	1.1.0 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗

1123.01q1System.2-01.q 01.05 Operating System Access Control

ID: 1123.01q1System.2-01.q Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit Windows machines that have extra accounts in the Administrators group ↗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗. Machines are non-compliant if the local Administrators group contains members that are not listed in the policy parameter.	auditIfNotExists	2.0.0 ↗
Authorize access to security functions and information ↗	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize and manage access ↗	CMA_0023 - Authorize and manage access	Manual, Disabled	1.1.0 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege 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 ↗

1124.01q1System.34-01.q 01.05 Operating System Access Control

ID: 1124.01q1System.34-01.q 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 ↗
Reissue authenticators for changed groups and accounts ↗	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	1.1.0 ↗

1125.01q2System.1-01.q 01.05 Operating System Access Control

ID: 1125.01q2System.1-01.q Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Adopt biometric authentication	CMA_0005 - Adopt biometric authentication mechanisms	Manual, Disabled	1.1.0 ↗

Mechanisms 	Description	Effect(s)	Version
(Azure portal) Audit Windows machines that have the specified members in the Administrators group 	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol . Machines are non-compliant if the local Administrators group contains one or more of the members listed in the policy parameter.	auditIfNotExists	(GitHub) 2.0.0 
Enforce user uniqueness 	CMA_0250 - Enforce user uniqueness	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 

1127.01q2System.3-01.q 01.05 Operating System Access Control

ID: 1127.01q2System.3-01.q Ownership: Shared

 Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Audit Windows machines missing any of specified members in the Administrators group 	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol . Machines are non-compliant if the local Administrators group does not contain one or more members that are listed in the policy parameter.	auditIfNotExists	2.0.0 
Distribute authenticators 	CMA_0184 - Distribute authenticators	Manual, Disabled	1.1.0 

1128.01q2System.5-01.q 01.05 Operating System Access Control

ID: 1128.01q2System.5-01.q 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 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗

1129.01v1System.12-01.v 01.06 Application and Information Access Control

ID: 1129.01v1System.12-01.v 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 ↗
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 ↗
Define information system account types ↗	CMA_0121 - Define information system account types	Manual, Disabled	1.1.0 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege 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 ↗
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 ↗

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 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↗

1130.01v2System.1-01.v 01.06 Application and Information Access Control

ID: 1130.01v2System.1-01.v Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign account managers ↗	CMA_0015 - Assign account managers	Manual, Disabled	1.1.0 ↗
Define information system account types ↗	CMA_0121 - Define information system account types	Manual, Disabled	1.1.0 ↗
Document access privileges ↗	CMA_0186 - Document access privileges	Manual, Disabled	1.1.0 ↗
Establish conditions for role membership ↗	CMA_0269 - Establish conditions for role membership	Manual, Disabled	1.1.0 ↗
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	1.1.0 ↗

1131.01v2System.2-01.v 01.06 Application and Information Access Control

ID: 1131.01v2System.2-01.v Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Control information flow ↗	CMA_0079 - Control information flow	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 ↗
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 ↗
Information flow control using security policy filters ↗	CMA_C1029 - Information flow control using security policy filters	Manual, Disabled	1.1.0 ↗

1132.01v2System.3-01.v 01.06 Application and Information Access Control

ID: 1132.01v2System.3-01.v Ownership: Shared

↔ [Expand table](#)

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 ↗
Protect special information ↗	CMA_0409 - Protect special information	Manual, Disabled	1.1.0 ↗

1133.01v2System.4-01.v 01.06 Application and Information Access Control

ID: 1133.01v2System.4-01.v 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 ↗

1134.01v3System.1-01.v 01.06 Application and Information Access Control

ID: 1134.01v3System.1-01.v Ownership: Shared

[Expand table](#)

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 ↗
Limit privileges to make changes in production environment ↗	CMA_C1206 - Limit privileges to make changes in production environment	Manual, Disabled	1.1.0 ↗
Protect special information ↗	CMA_0409 - Protect special information	Manual, Disabled	1.1.0 ↗

1135.02i1Organizational.1234-02.i 02.04 Termination or Change of Employment

ID: 1135.02i1Organizational.1234-02.i 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 ↗
Initiate transfer or reassignment actions ↗	CMA_0333 - Initiate transfer or reassignment actions	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Modify access authorizations upon personnel transfer ↗	CMA_0374 - Modify access authorizations upon personnel transfer	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 ↗
Reevaluate access upon personnel transfer ↗	CMA_0424 - Reevaluate access upon personnel transfer	Manual, Disabled	1.1.0 ↗
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	1.1.0 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗

1136.02i2Organizational.1-02.i 02.04 Termination or Change of Employment

ID: 1136.02i2Organizational.1-02.i 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 ↗
Disable user accounts posing a significant risk ↗	CMA_C1026 - Disable user accounts posing a significant risk	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)
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	1.1.0 ↗

1137.06e1Organizational.1-06.e 06.01 Compliance with Legal Requirements

ID: 1137.06e1Organizational.1-06.e 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 ↗
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	1.1.0 ↗
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	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 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0 ↗
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0 ↗

1139.01b1System.68-01.b 01.02 Authorized Access to Information Systems

ID: 1139.01b1System.68-01.b 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 ↗
Define information system account types ↗	CMA_0121 - Define information system account types	Manual, Disabled	1.1.0 ↗
Document access privileges ↗	CMA_0186 - Document access privileges	Manual, Disabled	1.1.0 ↗
Establish conditions for role membership ↗	CMA_0269 - Establish conditions for role membership	Manual, Disabled	1.1.0 ↗
Reissue authenticators for changed groups and accounts ↗	CMA_0426 - Reissue authenticators for changed groups and accounts	Manual, Disabled	1.1.0 ↗
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	1.1.0 ↗

1143.01c1System.123-01.c 01.02 Authorized Access to Information Systems

ID: 1143.01c1System.123-01.c 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 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege access	Manual, Disabled	1.1.0 ↗
Enforce mandatory and discretionary	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
access control policies ↗			
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 ↗
Monitor account activity ↗	CMA_0377 - Monitor account activity	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 ↗
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 ↗

1144.01c1System.4-01.c 01.02 Authorized Access to Information Systems

ID: 1144.01c1System.4-01.c 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 ↗
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 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ least privilege access ↗	CMA_0212 - Employ least privilege 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 ↗

1145.01c2System.1-01.c 01.02 Authorized Access to Information Systems

ID: 1145.01c2System.1-01.c 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 ↗
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 ↗
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 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	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 ↗
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↗

1146.01c2System.23-01.c 01.02 Authorized Access to Information Systems

ID: 1146.01c2System.23-01.c 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 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege 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 software execution privileges ↗	CMA_C1041 - Enforce software execution privileges	Manual, Disabled	1.1.0 ↗
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 ↗
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	1.1.0 ↗

1147.01c2System.456-01.c 01.02 Authorized Access to Information Systems

ID: 1147.01c2System.456-01.c 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 ↗
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 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege 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 ↗

1148.01c2System.78-01.c 01.02 Authorized Access to Information Systems

ID: 1148.01c2System.78-01.c Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Authorize access to security functions and information ↗	CMA_0022 - Authorize access to security functions and information	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Authorize and manage access ↗	CMA_0023 - Authorize and manage access	Manual, Disabled	1.1.0 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege 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 ↗
Restrict access to privileged accounts ↗	CMA_0446 - Restrict access to privileged accounts	Manual, Disabled	1.1.0 ↗
Windows machines should meet requirements for 'Security Options - Accounts' ↗	Windows machines should have the specified Group Policy settings in the category 'Security Options - Accounts' for limiting local account use of blank passwords and guest account status. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗

1150.01c2System.10-01.c 01.02 Authorized Access to Information Systems

ID: 1150.01c2System.10-01.c Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Control information flow ↗	CMA_0079 - Control information flow	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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↴
Information flow control using security policy filters ↴	CMA_C1029 - Information flow control using security policy filters	Manual, Disabled	1.1.0 ↴
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 ↴

1151.01c3System.1-01.c 01.02 Authorized Access to Information Systems

ID: 1151.01c3System.1-01.c 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 privileged functions ↴	CMA_0019 - Audit privileged functions	Manual, Disabled	1.1.0 ↴
Conduct a full text analysis of logged privileged commands ↴	CMA_0056 - Conduct a full text analysis of logged privileged commands	Manual, Disabled	1.1.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↗

1152.01c3System.2-01.c 01.02 Authorized Access to Information Systems

ID: 1152.01c3System.2-01.c 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 ↗
Conduct a full text analysis of logged privileged commands ↗	CMA_0056 - Conduct a full text analysis of logged privileged commands	Manual, Disabled	1.1.0 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege access	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 ↗
There should be more than one owner assigned to	It is recommended to designate more than one subscription owner	AuditIfNotExists, Disabled	3.0.0 ↗

Name	Description	Effect(s)	Version
(GitHub)			
your subscription ↗	in order to have administrator access redundancy.		
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↗

1153.01c3System.35-01.c 01.02 Authorized Access to Information Systems

ID: 1153.01c3System.35-01.c Ownership: Shared

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

Name	Description	Effect(s)	Version
(GitHub)			
Azure Role-Based Access Control (RBAC) should be used on Kubernetes Services ↗	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	1.0.3 ↗
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	1.1.0 ↗

1166.01e1System.12-01.e 01.02 Authorized Access to Information Systems

ID: 1166.01e1System.12-01.e Ownership: Shared

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

Name	Description	Effect(s)	Version
(GitHub)			
Audit user account status ↗	CMA_0020 - Audit user account status	Manual, Disabled	1.1.0 ↗
Initiate transfer or reassignment actions ↗	CMA_0333 - Initiate transfer or reassignment actions	Manual, Disabled	1.1.0 ↗
Modify access authorizations upon personnel transfer ↗	CMA_0374 - Modify access authorizations upon personnel	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	transfer		
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 ↗
Review account provisioning logs ↗	CMA_0460 - Review account provisioning logs	Manual, Disabled	1.1.0 ↗
Review user accounts ↗	CMA_0480 - Review user accounts	Manual, Disabled	1.1.0 ↗

1167.01e2System.1-01.e 01.02 Authorized Access to Information Systems

ID: 1167.01e2System.1-01.e Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Assign system identifiers ↗	CMA_0018 - Assign system identifiers	Manual, Disabled	1.1.0 ↗
Identify status of individual users ↗	CMA_C1316 - Identify status of individual users	Manual, Disabled	1.1.0 ↗

1168.01e2System.2-01.e 01.02 Authorized Access to Information Systems

ID: 1168.01e2System.2-01.e Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege access	Manual, Disabled	1.1.0 ↗
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 ↗

1175.01j1Organizational.8-01.j 01.04 Network Access Control

ID: 1175.01j1Organizational.8-01.j 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 ↗
Enforce user uniqueness ↗	CMA_0250 - Enforce user uniqueness	Manual, Disabled	1.1.0 ↗
Identify and authenticate network devices ↗	CMA_0296 - Identify and authenticate network devices	Manual, Disabled	1.1.0 ↗
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 ↗
Support personal verification credentials issued by legal authorities ↗	CMA_0507 - Support personal verification credentials issued by legal authorities	Manual, Disabled	1.1.0 ↗

1178.01j2Organizational.7-01.j 01.04 Network Access Control

ID: 1178.01j2Organizational.7-01.j Ownership: Shared

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

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 ↗
Enforce user uniqueness ↗	CMA_0250 - Enforce user uniqueness	Manual, Disabled	1.1.0 ↗
Require use of individual authenticators ↗	CMA_C1305 - Require use of individual authenticators	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 ↗

1179.01j3Organizational.1-01.j 01.04 Network Access Control

ID: 1179.01j3Organizational.1-01.j 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 ↗
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 ↗
Implement controls to secure alternate work sites ↗	CMA_0315 - Implement controls to secure alternate work sites	Manual, Disabled	1.1.0 ↗
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 ↗
Monitor access across the	CMA_0376 - Monitor access	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
organization ↗	across the organization		
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗

1192.01|1Organizational.1-01.| 01.04 Network Access Control

ID: 1192.01|1Organizational.1-01.| 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 ↗
Define a physical key management process ↗	CMA_0115 - Define a physical key management process	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 ↗
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 ↗

1193.01|2Organizational.13-01.| 01.04 Network Access Control

ID: 1193.01|2Organizational.13-01.| 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 ↗
Define a physical key management process ↗	CMA_0115 - Define a physical key management process	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 ↗
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 ↗

1194.01|2Organizational.2-01.I 01.04 Network Access Control

ID: 1194.01|2Organizational.2-01.I Ownership: Shared

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

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

1195.01|3Organizational.1-01.I 01.04 Network Access Control

ID: 1195.01|3Organizational.1-01.I Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)		(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 ↴

1197.01I3Organizational.3-01.I 01.04 Network Access Control

ID: 1197.01I3Organizational.3-01.I 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	3.0.0 ↴

12 Audit Logging & Monitoring

1201.06e1Organizational.2-06.e 06.01 Compliance with Legal Requirements

ID: 1201.06e1Organizational.2-06.e Ownership: Shared

[\[\]](#) Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Develop acceptable use policies and procedures ↴	CMA_0143 - Develop acceptable use policies and procedures	Manual, Disabled	1.1.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	1.1.0 ↗
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	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 ↗
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 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0 ↗
Provide privacy notice ↗	CMA_0414 - Provide privacy notice	Manual, Disabled	1.1.0 ↗
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0 ↗

1202.09aa1System.1-09.aa 09.10 Monitoring

ID: 1202.09aa1System.1-09.aa Ownership: Shared

[Expand table](#)

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Determine auditable events ↴	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↴
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 ↴
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 ↴
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	3.0.0 ↴

1203.09aa1System.2-09.aa 09.10 Monitoring

ID: 1203.09aa1System.2-09.aa Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure Azure Audit capabilities ↴	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	1.1.1 ↴
Determine auditable events ↴	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↴
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	5.1.0 ↴

1204.09aa1System.3-09.aa 09.10 Monitoring

ID: 1204.09aa1System.3-09.aa Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure Azure Audit capabilities ↗	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	1.1.1 ↗
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↗
Monitor account activity ↗	CMA_0377 - Monitor account activity	Manual, Disabled	1.1.0 ↗
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	3.1.0 ↗

1205.09aa2System.1-09.aa 09.10 Monitoring

ID: 1205.09aa2System.1-09.aa Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure Azure Audit capabilities ↗	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	1.1.1 ↗
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↗
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 ↗
Provide capability to process customer-controlled audit records ↗	CMA_C1126 - Provide capability to process customer-controlled audit records	Manual, Disabled	1.1.0 ↗
Resource logs in Batch accounts should	Audit enabling of resource logs. This enables you to recreate activity trails to	AuditIfNotExists, Disabled	5.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
be enabled ↗	use for investigation purposes; when a security incident occurs or when your network is compromised		

1206.09aa2System.23-09.aa 09.10 Monitoring

ID: 1206.09aa2System.23-09.aa Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Configure Azure Audit capabilities ↗	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	1.1.1 ↗
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↗
Employ automatic shutdown/restart when violations are detected ↗	CMA_C1715 - Employ automatic shutdown/restart when violations are detected	Manual, Disabled	1.1.0 ↗
Prohibit binary/machine-executable code ↗	CMA_C1717 - Prohibit binary/machine-executable code	Manual, Disabled	1.1.0 ↗
Verify software, firmware and information integrity ↗	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

1207.09aa2System.4-09.aa 09.10 Monitoring

ID: 1207.09aa2System.4-09.aa 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)
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 ↗
Configure Azure Audit capabilities ↗	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	1.1.1 ↗
Determine auditable events ↗	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↗
Enable dual or joint authorization ↗	CMA_0226 - Enable dual or joint authorization	Manual, Disabled	1.1.0 ↗
Govern and monitor audit processing activities ↗	CMA_0289 - Govern and monitor audit processing activities	Manual, Disabled	1.1.0 ↗
Protect audit information ↗	CMA_0401 - Protect audit information	Manual, Disabled	1.1.0 ↗
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	5.0.0 ↗
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	5.0.0 ↗
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 audit data ↗	CMA_0466 - Review audit data	Manual, Disabled	1.1.0 ↗

1208.09aa3System.1-09.aa 09.10 Monitoring

ID: 1208.09aa3System.1-09.aa Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit user account status ↗	CMA_0020 - Audit user account status	Manual, Disabled	1.1.0 ↗
Automate account management ↗	CMA_0026 - Automate account management	Manual, Disabled	1.1.0 ↗
Conduct a security impact analysis ↗	CMA_0057 - Conduct a security impact analysis	Manual, Disabled	1.1.0 ↗
Configure Azure Audit capabilities ↗	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	1.1.1 ↗
Determine auditable events ↗	CMA_0137 - Determine auditable events	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 developers ↗	CMA_0270 - Establish configuration management requirements for developers	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 ↗
Notify when account is not needed ↗	CMA_0383 - Notify when account is not needed	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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Perform audit for configuration change control ↴	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↴
Resource logs in Search services 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 ↴
Resource logs in Service Bus 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 ↴
Verify software, firmware and information integrity ↴	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0 ↴

1209.09aa3System.2-09.aa 09.10 Monitoring

ID: 1209.09aa3System.2-09.aa Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↴
Configure Azure Audit capabilities ↴	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	1.1.1 ↴
Determine auditable events ↴	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0 ↴

1210.09aa3System.3-09.aa 09.10 Monitoring

ID: 1210.09aa3System.3-09.aa 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
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
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
Determine auditable events	CMA_0137 - Determine auditable events	Manual, Disabled	1.1.0
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	5.0.0
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 and update the events defined in AU-02	CMA_C1106 - Review and update the events defined in AU-02	Manual, Disabled	1.1.0
Review audit data	CMA_0466 - Review audit data	Manual, Disabled	1.1.0
Use system clocks for audit records	CMA_0535 - Use system clocks for audit records	Manual, Disabled	1.1.0

12100.09ab2System.15-09.ab 09.10 Monitoring

ID: 12100.09ab2System.15-09.ab 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 ↗
Document wireless access security controls ↗	CMA_C1695 - Document wireless access security controls	Manual, Disabled	1.1.0 ↗
Virtual machines should have the Log Analytics extension installed ↗	This policy audits any Windows/Linux virtual machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1 ↗

12101.09ab1Organizational.3-09.ab 09.10 Monitoring

ID: 12101.09ab1Organizational.3-09.ab 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	1.1.0 ↗
Correlate audit records ↗	CMA_0087 - Correlate audit records	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 ↗
Establish requirements for audit review and reporting ↗	CMA_0277 - Establish requirements for audit review and reporting	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 activity	Manual, Disabled	1.1.0 🔗
Review role group changes weekly 🔗	CMA_0476 - Review role group changes weekly	Manual, Disabled	1.1.0 🔗
Specify permitted actions associated with customer audit information 🔗	CMA_C1122 - Specify permitted actions associated with customer audit information	Manual, Disabled	1.1.0 🔗
The Log Analytics extension should be installed on Virtual Machine Scale Sets 🔗	This policy audits any Windows/Linux Virtual Machine Scale Sets if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1 🔗
Update information security policies 🔗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 🔗

12102.09ab1Organizational.4-09.ab 09.10 Monitoring

ID: 12102.09ab1Organizational.4-09.ab Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit Windows machines on which the Log Analytics agent is	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol 🔗 . Machines are non-compliant if the agent is not installed, or if it is installed but the COM object	auditIfNotExists	2.0.0 🔗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
not connected as expected ↗	AgentConfigManager.MgmtSvcCfg returns that it is registered to a workspace other than the ID specified in the policy parameter.		
Conduct incident response testing ↗	CMA_0060 - Conduct incident response testing	Manual, Disabled	1.1.0 ↗
Develop POA&M ↗	CMA_C1156 - Develop POA&M	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 ↗
Select additional testing for security control assessments ↗	CMA_C1149 - Select additional testing for security control assessments	Manual, Disabled	1.1.0 ↗
Update POA&M items ↗	CMA_C1157 - Update POA&M items	Manual, Disabled	1.1.0 ↗

12103.09ab1Organizational.5-09.ab 09.10 Monitoring

ID: 12103.09ab1Organizational.5-09.ab 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 activity	Manual, Disabled	1.1.0 ↗
Review role group changes weekly ↗	CMA_0476 - Review role group changes weekly	Manual, Disabled	1.1.0 ↗

1211.09aa3System.4-09.aa 09.10 Monitoring

ID: 1211.09aa3System.4-09.aa 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 ↗
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 ↗
Establish and document change control processes ↗	CMA_0265 - Establish and document change control processes	Manual, Disabled	1.1.0 ↗
Establish configuration	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
management requirements for developers ↗			
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗
Perform disposition review ↗	CMA_0391 - Perform disposition review	Manual, Disabled	1.1.0 ↗
Resource logs in Azure Key Vault Managed HSM should be enabled ↗	To recreate activity trails for investigation purposes when a security incident occurs or when your network is compromised, you may want to audit by enabling resource logs on Managed HSMs. Please follow the instructions here: https://docs.microsoft.com/azure/key-vault/managed-hsm/logging .	AuditIfNotExists, Disabled	1.1.0 ↗
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	5.0.0 ↗
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 ↗

1212.09ab1System.1-09.ab 09.10 Monitoring

ID: 1212.09ab1System.1-09.ab Ownership: Shared

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Monitor log profile should collect logs for categories 'write,' 'delete,' and 'action' ↗	This policy ensures that a log profile collects logs for categories 'write,' 'delete,' and 'action'	AuditIfNotExists, Disabled	1.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Obtain legal opinion for monitoring system activities ↴	CMA_C1688 - Obtain legal opinion for monitoring system activities	Manual, Disabled	1.1.0 ↴
Provide monitoring information as needed ↴	CMA_C1689 - Provide monitoring information as needed	Manual, Disabled	1.1.0 ↴

1213.09ab2System.128-09.ab 09.10 Monitoring

ID: 1213.09ab2System.128-09.ab 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 ↴
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 ↴
Route traffic through managed network access points ↴	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	1.1.0 ↴

1214.09ab2System.3456-09.ab 09.10 Monitoring

ID: 1214.09ab2System.3456-09.ab 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 ↗
Azure Monitor should collect activity logs from all regions ↗	This policy audits the Azure Monitor log profile which does not export activities from all Azure supported regions including global.	AuditIfNotExists, Disabled	2.0.0 ↗
Conduct a full text analysis of logged privileged commands ↗	CMA_0056 - Conduct a full text analysis of logged privileged commands	Manual, Disabled	1.1.0 ↗
Configure Azure Audit capabilities ↗	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	1.1.1 ↗
Determine auditable events ↗	CMA_0137 - Determine auditable events	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 ↗
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↗

1215.09ab2System.7-09.ab 09.10 Monitoring

ID: 1215.09ab2System.7-09.ab 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	CMA_C1124 - Provide audit review, analysis, and reporting capability	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
capability ↗			
Provide capability to process customer-controlled audit records ↗	CMA_C1126 - Provide capability to process customer-controlled audit records	Manual, Disabled	1.1.0 ↗
Virtual machines should have the Log Analytics extension installed ↗	This policy audits any Windows/Linux virtual machines if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1 ↗

1216.09ab3System.12-09.ab 09.10 Monitoring

ID: 1216.09ab3System.12-09.ab 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 ↗
Configure Azure Audit capabilities ↗	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	1.1.1 ↗
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 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	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 ↗
Integrate audit review, analysis, and reporting ↗	CMA_0339 - Integrate audit review, analysis, and reporting	Manual, Disabled	1.1.0 ↗
Integrate cloud app security	CMA_0340 - Integrate cloud app	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
with a siem ↗	security with a siem		
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 and update the events defined in AU-02 ↗	CMA_C1106 - Review and update the events defined in AU-02	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 activity	Manual, Disabled	1.1.0 ↗
Review role group changes weekly ↗	CMA_0476 - Review role group changes weekly	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 ↗
The Log Analytics extension should be installed on Virtual Machine Scale Sets ↗	This policy audits any Windows/Linux Virtual Machine Scale Sets if the Log Analytics extension is not installed.	AuditIfNotExists, Disabled	1.0.1 ↗
Turn on sensors for endpoint security solution ↗	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	1.1.0 ↗

1217.09ab3System.3-09.ab 09.10 Monitoring

ID: 1217.09ab3System.3-09.ab 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 
Audit Windows machines on which the Log Analytics agent is not connected as expected 🔗	Requires that prerequisites are deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol  . Machines are non-compliant if the agent is not installed, or if it is installed but the COM object AgentConfigManager.MgmtSvcCfg returns that it is registered to a workspace other than the ID specified in the policy parameter.	auditIfNotExists	2.0.0 
Develop an incident response plan 🔗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 
Document wireless access security controls 🔗	CMA_C1695 - Document wireless access security controls	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 

1218.09ab3System.47-09.ab 09.10 Monitoring

ID: 1218.09ab3System.47-09.ab 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 
Authorize, monitor, and control voip 🔗	CMA_0025 - Authorize, monitor, and control voip	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)
Document security operations ↗	CMA_0202 - Document security operations	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 ↗
Turn on sensors for endpoint security solution ↗	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	1.1.0 ↗

1219.09ab3System.10-09.ab 09.10 Monitoring

ID: 1219.09ab3System.10-09.ab Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Monitor log profile should collect logs for categories 'write,' 'delete,' and 'action' ↗	This policy ensures that a log profile collects logs for categories 'write,' 'delete,' and 'action'	AuditIfNotExists, Disabled	1.0.0 ↗
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 ↗
Provide capability to process customer-controlled audit records ↗	CMA_C1126 - Provide capability to process customer-controlled audit records	Manual, Disabled	1.1.0 ↗

1220.09ab3System.56-09.ab 09.10 Monitoring

ID: 1220.09ab3System.56-09.ab 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
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
Route traffic through managed network access points	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	1.1.0
Verify software, firmware and information integrity	CMA_0542 - Verify software, firmware and information integrity	Manual, Disabled	1.1.0
View and configure system diagnostic data	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0

1222.09ab3System.8-09.ab 09.10 Monitoring

ID: 1222.09ab3System.8-09.ab **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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Correlate audit records ↗	CMA_0087 - Correlate audit records	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Disseminate security alerts to personnel ↗	CMA_C1705 - Disseminate security alerts to personnel	Manual, Disabled	1.1.0 ↗
Establish a threat intelligence program ↗	CMA_0260 - Establish a threat intelligence program	Manual, Disabled	1.1.0 ↗
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 ↗
Integrate cloud app security with a siem ↗	CMA_0340 - Integrate cloud app security with a siem	Manual, Disabled	1.1.0 ↗
Provide capability to process customer-controlled audit records ↗	CMA_C1126 - Provide capability to process customer-controlled audit records	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 ↗

1229.09c1Organizational.1-09.c 09.01 Documented Operating Procedures

ID: 1229.09c1Organizational.1-09.c Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Role-Based Access Control (RBAC) should be used on Kubernetes Services ↗	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	1.0.3 ↗

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 ↗

1230.09c2Organizational.1-09.c 09.01 Documented Operating Procedures

ID: 1230.09c2Organizational.1-09.c 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 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 ↗
Audit user account status ↗	CMA_0020 - Audit user account status	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 ↗
Configure Azure Audit capabilities ↗	CMA_C1108 - Configure Azure Audit capabilities	Manual, Disabled	1.1.1 ↗
Determine auditable events ↗	CMA_0137 - Determine auditable events	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 ↗
Enforce mandatory and discretionary access control policies ↗	CMA_0246 - Enforce mandatory and discretionary access control policies	Manual, Disabled	1.1.0 ↗
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	1.1.0 ↗
Review audit data ↗	CMA_0466 - Review audit data	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 ↗
Separate duties of individuals ↗	CMA_0492 - Separate duties of individuals	Manual, Disabled	1.1.0 ↗

1231.09c2Organizational.23-09.c 09.01 Documented Operating Procedures

ID: 1231.09c2Organizational.23-09.c 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 ↗

1232.09c3Organizational.12-09.c 09.01 Documented Operating Procedures

ID: 1232.09c3Organizational.12-09.c 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 ↗
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 a full text analysis of logged privileged commands ↗	CMA_0056 - Conduct a full text analysis of logged privileged commands	Manual, Disabled	1.1.0 ↗
Define access authorizations to support separation of duties ↗	CMA_0116 - Define access authorizations to support separation of duties	Manual, Disabled	1.1.0 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Document separation of duties ↗	CMA_0204 - Document separation of duties	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege access	Manual, Disabled	1.1.0 ↗
Enable dual or joint authorization ↗	CMA_0226 - Enable dual or joint authorization	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 software execution privileges ↗	CMA_C1041 - Enforce software execution privileges	Manual, Disabled	1.1.0 ↗
Monitor privileged role assignment ↗	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	1.1.0 ↗
Protect audit	CMA_0401 - Protect audit information	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
information ↗		Disabled	
Reassign or remove user privileges as needed ↗	CMA_C1040 - Reassign or remove user privileges as needed	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 user privileges ↗	CMA_C1039 - Review user privileges	Manual, Disabled	1.1.0 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗
Separate duties of individuals ↗	CMA_0492 - Separate duties of individuals	Manual, Disabled	1.1.0 ↗
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↗
Windows machines should meet requirements for 'User Rights Assignment' ↗	Windows machines should have the specified Group Policy settings in the category 'User Rights Assignment' for allowing log on locally, RDP, access from the network, and many other user activities. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗

1233.09c3Organizational.3-09.c 09.01 Documented Operating Procedures

ID: 1233.09c3Organizational.3-09.c 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 ↗

1270.09ad1System.12-09.ad 09.10 Monitoring

ID: 1270.09ad1System.12-09.ad Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An activity log alert should exist for specific Administrative operations ↴	This policy audits specific Administrative operations with no activity log alerts configured.	AuditIfNotExists, Disabled	1.0.0 ↗
Audit privileged functions ↴	CMA_0019 - Audit privileged functions	Manual, Disabled	1.1.0 ↗
Conduct a full text analysis of logged privileged commands ↴	CMA_0056 - Conduct a full text analysis of logged privileged commands	Manual, Disabled	1.1.0 ↗
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 ↗
Monitor privileged role assignment ↴	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	1.1.0 ↗

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 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 activity	Manual, Disabled	1.1.0 ↴
Review role group changes weekly ↴	CMA_0476 - Review role group changes weekly	Manual, Disabled	1.1.0 ↴
Revoke privileged roles as appropriate ↴	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↴
Use privileged identity management ↴	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↴

1271.09ad1System.1-09.ad 09.10 Monitoring

ID: 1271.09ad1System.1-09.ad Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An activity log alert should exist for specific Administrative operations ↴	This policy audits specific Administrative operations with no activity log alerts configured.	AuditIfNotExists, Disabled	1.0.0 ↴
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)
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Document separation of duties ↗	CMA_0204 - Document separation of duties	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege access	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 ↗
Separate duties of individuals ↗	CMA_0492 - Separate duties of individuals	Manual, Disabled	1.1.0 ↗

1271.09ad2System.1 09.10 Monitoring

ID: 1271.09ad2System.1 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 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Document separation of duties ↗	CMA_0204 - Document separation of duties	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege access	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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Separate duties of individuals ↗	CMA_0492 - Separate duties of individuals	Manual, Disabled	1.1.0 ↗

1276.09c2Organizational.2-09.c 09.01 Documented Operating Procedures

ID: 1276.09c2Organizational.2-09.c 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 ↗
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 a full text analysis of logged privileged commands ↗	CMA_0056 - Conduct a full text analysis of logged privileged commands	Manual, Disabled	1.1.0 ↗
Define access authorizations to support separation of duties ↗	CMA_0116 - Define access authorizations to support separation of duties	Manual, Disabled	1.1.0 ↗
Design an access control model ↗	CMA_0129 - Design an access control model	Manual, Disabled	1.1.0 ↗
Document separation of duties ↗	CMA_0204 - Document separation of duties	Manual, Disabled	1.1.0 ↗
Employ least privilege access ↗	CMA_0212 - Employ least privilege 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 software execution privileges ↗	CMA_C1041 - Enforce software execution privileges	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Monitor privileged role assignment ↗	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	1.1.0 ↗
Protect audit information ↗	CMA_0401 - Protect audit information	Manual, Disabled	1.1.0 ↗
Reassign or remove user privileges as needed ↗	CMA_C1040 - Reassign or remove user privileges as needed	Manual, Disabled	1.1.0 ↗
Require approval for account creation ↗	CMA_0431 - Require approval for account creation	Manual, Disabled	1.1.0 ↗
Review user privileges ↗	CMA_C1039 - Review user privileges	Manual, Disabled	1.1.0 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗
Separate duties of individuals ↗	CMA_0492 - Separate duties of individuals	Manual, Disabled	1.1.0 ↗
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↗

1277.09c2Organizational.4-09.c 09.01 Documented Operating Procedures

ID: 1277.09c2Organizational.4-09.c 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Windows machines should meet requirements for 'Security Options - User Account Control' ↴	Windows machines should have the specified Group Policy settings in the category 'Security Options - User Account Control' for mode for admins, behavior of elevation prompt, and virtualizing file and registry write failures. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↴.	AuditIfNotExists, Disabled	3.0.0 ↴

1278.09c2Organizational.56-09.c 09.01 Documented Operating Procedures

ID: 1278.09c2Organizational.56-09.c 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 ↴

1279.09c3Organizational.4-09.c 09.01 Documented Operating Procedures

ID: 1279.09c3Organizational.4-09.c 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	Manual, Disabled	1.1.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	of duties		
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 

13 Education, Training and Awareness

1301.02e1Organizational.12-02.e 02.03 During Employment

ID: 1301.02e1Organizational.12-02.e 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 
Develop organization code of conduct policy 	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	1.1.0 
Document personnel acceptance of privacy requirements 	CMA_0193 - Document personnel acceptance of privacy requirements	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 
Prohibit unfair practices 	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0 
Provide periodic role-based security training 	CMA_C1095 - Provide periodic role-based security training	Manual, Disabled	1.1.0 
Provide periodic security awareness training 	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 
Provide role-based practical exercises 	CMA_C1096 - Provide role-based practical exercises	Manual, Disabled	1.1.0 

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide role-based security training ↗	CMA_C1094 - Provide role-based security training	Manual, Disabled	1.1.0 ↗
Provide role-based training on suspicious activities ↗	CMA_C1097 - Provide role-based training on suspicious activities	Manual, Disabled	1.1.0 ↗
Provide security awareness training for insider threats ↗	CMA_0417 - Provide security awareness training for insider threats	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 ↗
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0 ↗

1302.02e2Organizational.134-02.e 02.03 During Employment

ID: 1302.02e2Organizational.134-02.e 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 ↗
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	1.1.0 ↗

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 ↗
Document security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	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 ↗
Implement a threat awareness program ↗	CMA_C1758 - Implement a threat awareness program	Manual, Disabled	1.1.0 ↗
Implement an insider threat program ↗	CMA_C1751 - Implement an insider threat program	Manual, Disabled	1.1.0 ↗
Monitor security and privacy training completion ↗	CMA_0379 - Monitor security and privacy training completion	Manual, Disabled	1.1.0 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0 ↗
Provide periodic security awareness training ↗	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗
Provide security awareness training for insider threats ↗	CMA_0417 - Provide security awareness training for insider threats	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 ↗
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Update rules of behavior and access agreements every 3 years	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0

1303.02e2Organizational.2-02.e 02.03 During Employment

ID: 1303.02e2Organizational.2-02.e 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
Develop organization code of conduct policy	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	1.1.0
Document personnel acceptance of privacy requirements	CMA_0193 - Document personnel acceptance of privacy requirements	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
Prohibit unfair practices	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0
Review and sign revised rules of behavior	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0
Update rules of behavior and access agreements	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0
Update rules of behavior and access agreements every 3 years	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0

1304.02e3Organizational.1-02.e 02.03 During Employment

ID: 1304.02e3Organizational.1-02.e 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 ↗
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗
Provide periodic role-based security training ↗	CMA_C1095 - Provide periodic role-based security training	Manual, Disabled	1.1.0 ↗
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 ↗
Require developers to provide training ↗	CMA_C1611 - Require developers to provide training	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 ↗

1305.02e3Organizational.23-02.e 02.03 During Employment

ID: 1305.02e3Organizational.23-02.e 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Retain training records ↗	CMA_0456 - Retain training records	Manual, Disabled	1.1.0 ↗

1306.06e1Organizational.5-06.e 06.01 Compliance with Legal Requirements

ID: 1306.06e1Organizational.5-06.e 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 ↗
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	1.1.0 ↗
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	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 ↗
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 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0 ↗
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0 ↗

1307.07c1Organizational.124-07.c 07.01 Responsibility for Assets

ID: 1307.07c1Organizational.124-07.c 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 ↗
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	1.1.0 ↗
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	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 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0 ↗
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Update information security policies ↗	CMA_0518 - Update information security policies	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0 ↗

1308.09j1Organizational.5-09.j 09.04 Protection Against Malicious and Mobile Code

ID: 1308.09j1Organizational.5-09.j 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 ↗
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	1.1.0 ↗
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	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 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	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 and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Review threat protection status weekly ↗	CMA_0479 - Review threat protection status weekly	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0 ↗

1309.01x1System.36-01.x 01.07 Mobile Computing and Teleworking

ID: 1309.01x1System.36-01.x 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 periodic security awareness training ↗	CMA_C1091 - Provide periodic security awareness 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 ↗

1310.01y1Organizational.9-01.y 01.07 Mobile Computing and Teleworking

ID: 1310.01y1Organizational.9-01.y 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 periodic security awareness training ↗	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗
Provide role-based practical exercises ↗	CMA_C1096 - Provide role-based practical exercises	Manual, Disabled	1.1.0 ↗
Provide role-based security training ↗	CMA_C1094 - Provide role-based security training	Manual, Disabled	1.1.0 ↗
Provide role-based training on suspicious activities ↗	CMA_C1097 - Provide role-based training on suspicious activities	Manual, Disabled	1.1.0 ↗

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 ↗
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 ↗

1311.12c2Organizational.3-12.c 12.01 Information Security Aspects of Business Continuity Management

ID: 1311.12c2Organizational.3-12.c Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Incorporate simulated contingency training ↗	CMA_C1260 - Incorporate simulated contingency training	Manual, Disabled	1.1.0 ↗
Provide contingency training ↗	CMA_0412 - Provide contingency training	Manual, Disabled	1.1.0 ↗
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗

1313.02e1Organizational.3-02.e 02.03 During Employment

ID: 1313.02e1Organizational.3-02.e 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗
Provide periodic role-based security training ↗	CMA_C1095 - Provide periodic role-based security training	Manual, Disabled	1.1.0 ↗

1314.02e2Organizational.5-02.e 02.03 During Employment

ID: 1314.02e2Organizational.5-02.e 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 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	1.1.0 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy training	Manual, Disabled	1.1.0 ↗

1315.02e2Organizational.67-02.e 02.03 During Employment

ID: 1315.02e2Organizational.67-02.e 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 periodic security awareness training ↗	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 ↗

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 ↗

1324.07c1Organizational.3-07.c 07.01 Responsibility for Assets

ID: 1324.07c1Organizational.3-07.c Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	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 security and privacy training activities ↗	CMA_0198 - Document security and privacy training activities	Manual, Disabled	1.1.0 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0 ↗
Provide periodic role-based security training ↗	CMA_C1095 - Provide periodic role-based security training	Manual, Disabled	1.1.0 ↗
Review and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0 ↗

1325.09s1Organizational.3-09.s 09.08 Exchange of Information

ID: 1325.09s1Organizational.3-09.s Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop organization code of conduct policy ↗	CMA_0159 - Develop organization code of conduct policy	Manual, Disabled	1.1.0 ↗
Document personnel acceptance of privacy requirements ↗	CMA_0193 - Document personnel acceptance of privacy requirements	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 ↗
Prohibit unfair practices ↗	CMA_0396 - Prohibit unfair practices	Manual, Disabled	1.1.0 ↗
Provide periodic security awareness training ↗	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 ↗
Provide privacy training ↗	CMA_0415 - Provide privacy 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 and sign revised rules of behavior ↗	CMA_0465 - Review and sign revised rules of behavior	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements ↗	CMA_0521 - Update rules of behavior and access agreements	Manual, Disabled	1.1.0 ↗
Update rules of behavior and access agreements every 3 years ↗	CMA_0522 - Update rules of behavior and access agreements every 3 years	Manual, Disabled	1.1.0 ↗

1327.02e2Organizational.8-02.e 02.03 During Employment

ID: 1327.02e2Organizational.8-02.e 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 ↗
Provide periodic security awareness training ↗	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 ↗
Provide security awareness training for insider threats ↗	CMA_0417 - Provide security awareness training for insider threats	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 ↗

1331.02e3Organizational.4-02.e 02.03 During Employment

ID: 1331.02e3Organizational.4-02.e 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 ↗
Incorporate simulated events into incident response training ↗	CMA_C1356 - Incorporate simulated events into incident response training	Manual, Disabled	1.1.0 ↗
Install an alarm system ↗	CMA_0338 - Install an alarm system	Manual, Disabled	1.1.0 ↗
Manage a secure surveillance camera system ↗	CMA_0354 - Manage a secure surveillance camera system	Manual, Disabled	1.1.0 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗

1334.02e2Organizational.12-02.e 02.03 During Employment

ID: 1334.02e2Organizational.12-02.e 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 ↗
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 ↗

1336.02e1Organizational.5-02.e 02.03 During Employment

ID: 1336.02e1Organizational.5-02.e 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 periodic security awareness training ↗	CMA_C1091 - Provide periodic security awareness training	Manual, Disabled	1.1.0 ↗
Provide role-based practical exercises ↗	CMA_C1096 - Provide role-based practical exercises	Manual, Disabled	1.1.0 ↗
Provide role-based training on suspicious activities ↗	CMA_C1097 - Provide role-based training on suspicious activities	Manual, Disabled	1.1.0 ↗
Provide security awareness training for insider threats ↗	CMA_0417 - Provide security awareness training for insider threats	Manual, Disabled	1.1.0 ↗
Provide security training before providing access ↗	CMA_0418 - Provide security training before providing access	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide updated security awareness training ↗	CMA_C1090 - Provide updated security awareness training	Manual, Disabled	1.1.0 ↗

14 Third Party Assurance

1404.05i2Organizational.1-05.i 05.02 External Parties

ID: 1404.05i2Organizational.1-05.i 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 ↗

1406.05k1Organizational.110-05.k 05.02 External Parties

ID: 1406.05k1Organizational.110-05.k 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 ↗
Document protection of security information in acquisition contracts ↗	CMA_0195 - Document protection of security information in acquisition contracts	Manual, Disabled	1.1.0 ↗

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

1407.05k2Organizational.1-05.k 05.02 External Parties

ID: 1407.05k2Organizational.1-05.k 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	1.1.0 ↗
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	Manual, Disabled	1.1.0 ↗
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	Manual, Disabled	1.1.0 ↗

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

1408.09e1System.1-09.e 09.02 Control Third Party Service Delivery

ID: 1408.09e1System.1-09.e 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 ↗
Require interconnection security agreements ↗	CMA_C1151 - Require interconnection security agreements	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 ↗
Update interconnection security agreements ↗	CMA_0519 - Update interconnection security agreements	Manual, Disabled	1.1.0 ↗

1409.09e2System.1-09.e 09.02 Control Third Party Service Delivery

ID: 1409.09e2System.1-09.e 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 ↗
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 ↗
Document third-party personnel security requirements ↗	CMA_C1531 - Document third-party personnel security requirements	Manual, Disabled	1.1.0 ↗
Establish third-party personnel	CMA_C1529 - Establish third-party	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
security requirements ↗	personnel security requirements	Disabled	
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	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 ↗

1410.09e2System.23-09.e 09.02 Control Third Party Service Delivery

ID: 1410.09e2System.23-09.e 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 ↗
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 ↗

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 ↗

1411.09f1System.1-09.f 09.02 Control Third Party Service Delivery

ID: 1411.09f1System.1-09.f 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 ↗
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 ↗
Disseminate security alerts to personnel ↗	CMA_C1705 - Disseminate security alerts to personnel	Manual, Disabled	1.1.0 ↗
Document wireless access security controls ↗	CMA_C1695 - Document wireless access security controls	Manual, Disabled	1.1.0 ↗
Establish a threat intelligence program ↗	CMA_0260 - Establish a threat intelligence program	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 ↗

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	1.1.0 ↗
Route traffic through managed network access points ↗	CMA_0484 - Route traffic through managed network access points	Manual, Disabled	1.1.0 ↗
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	1.1.0 ↗

1416.10I1Organizational.1-10.I 10.05 Security In Development and Support Processes

ID: 1416.10I1Organizational.1-10.I 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 ↗
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 ↗

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 ↗

1417.10I2Organizational.1-10.I 10.05 Security In Development and Support Processes

ID: 1417.10I2Organizational.1-10.I 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 ↗
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	CMA_0199 - Document security assurance requirements in	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
contracts ↗	acquisition contracts		
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 ↗
Require developers to produce evidence of security assessment plan execution ↗	CMA_C1602 - Require developers to produce evidence of security assessment plan execution	Manual, Disabled	1.1.0 ↗

1419.05j1Organizational.12-05.j 05.02 External Parties

ID: 1419.05j1Organizational.12-05.j 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 ↗
Document protection of security information in acquisition	CMA_0195 - Document protection of security information in acquisition	Manual, Disabled	1.1.0 ↗

Contracts ↗	Contracts	Effect(s)	Version
(Azure portal) Document requirements for the use of shared data in contracts ↗	CMA_0197 - Document requirements for the use of shared data in contracts	Manual, Disabled	(GitHub) 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 ↗

1421.05j2Organizational.12-05.j 05.02 External Parties

ID: 1421.05j2Organizational.12-05.j Ownership: Shared

⋮ Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(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 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 ↗

1422.05j2Organizational.3-05.j 05.02 External Parties

ID: 1422.05j2Organizational.3-05.j 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 ↗
Identify external service providers ↗	CMA_C1591 - Identify external service providers	Manual, Disabled	1.1.0 ↗
Obtain approvals for acquisitions and outsourcing ↗	CMA_C1590 - Obtain approvals for acquisitions and outsourcing	Manual, Disabled	1.1.0 ↗

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	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 ↗

1423.05j2Organizational.4-05.j 05.02 External Parties

ID: 1423.05j2Organizational.4-05.j Ownership: Shared

expand table Expand table

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 boundary protection to isolate information systems ↗	CMA_C1639 - Employ boundary protection to isolate information systems	Manual, Disabled	1.1.0 ↗
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 ↗
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 ↗
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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	1.1.0 ↗
Verify security controls for external information systems ↗	CMA_0541 - Verify security controls for external information systems	Manual, Disabled	1.1.0 ↗

1424.05j2Organizational.5-05.j 05.02 External Parties

ID: 1424.05j2Organizational.5-05.j Ownership: Shared

[] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Accept only FICAM-approved third-party credentials ↗	CMA_C1348 - Accept only FICAM-approved third-party credentials	Manual, Disabled	1.1.0 ↗
Accept PIV credentials ↗	CMA_C1347 - Accept PIV credentials	Manual, Disabled	1.1.0 ↗
Conform to FICAM-issued profiles ↗	CMA_C1350 - Conform to FICAM-issued profiles	Manual, Disabled	1.1.0 ↗
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 ↗
Enforce user uniqueness ↗	CMA_0250 - Enforce user uniqueness	Manual, Disabled	1.1.0 ↗
Identify and authenticate non-organizational users ↗	CMA_C1346 - Identify and authenticate non-organizational users	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 ↗
Verify identity before distributing authenticators ↗	CMA_0538 - Verify identity before distributing authenticators	Manual, Disabled	1.1.0 ↗

1429.05k1Organizational.34-05.k 05.02 External Parties

ID: 1429.05k1Organizational.34-05.k 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 ↗
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 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 ↗
Document third-party personnel security requirements ↗	CMA_C1531 - Document third-party personnel security requirements	Manual, Disabled	1.1.0 ↗
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	Manual, Disabled	1.1.0 ↗
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	Manual, Disabled	1.1.0 ↗

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

1430.05k1Organizational.56-05.k 05.02 External Parties

ID: 1430.05k1Organizational.56-05.k 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 ↗
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 the information system environment in acquisition contracts ↗	CMA_0205 - Document the information system environment in acquisition contracts	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Document third-party personnel security requirements ↗	CMA_C1531 - Document third-party personnel security requirements	Manual, Disabled	1.1.0 ↗
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	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 ↗

1431.05k1Organizational.7-05.k 05.02 External Parties

ID: 1431.05k1Organizational.7-05.k 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	1.1.0 ↗
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	Manual, Disabled	1.1.0 ↗
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	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 ↗

1432.05k1Organizational.89-05.k 05.02 External Parties

ID: 1432.05k1Organizational.89-05.k 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 ↗
Document third-party personnel security requirements ↗	CMA_C1531 - Document third-party personnel security requirements	Manual, Disabled	1.1.0 ↗
Establish privacy requirements for contractors and service providers ↗	CMA_C1810 - Establish privacy requirements for contractors and service providers	Manual, Disabled	1.1.0 ↗
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	Manual, Disabled	1.1.0 ↗
Implement personnel screening ↗	CMA_0322 - Implement personnel screening	Manual, Disabled	1.1.0 ↗
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	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 ↗

1438.09e2System.4-09.e 09.02 Control Third Party Service Delivery

ID: 1438.09e2System.4-09.e 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 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 external providers consistently meet interests of the customers ↗	CMA_C1592 - Ensure external providers consistently meet interests of the customers	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 ↗

1450.05i2Organizational.2-05.i 05.02 External Parties

ID: 1450.05i2Organizational.2-05.i 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 ↗
Define and document government oversight ↗	CMA_C1587 - Define and document government oversight	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 ↗
Enforce SSL connection should be enabled for PostgreSQL database servers ↗	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	1.0.1 ↗
Establish policies for supply chain risk management ↗	CMA_0275 - Establish policies for supply chain risk management	Manual, Disabled	1.1.0 ↗
Identify incident response personnel ↗	CMA_0301 - Identify incident response personnel	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	CMA_0515 - Undergo independent security review	Manual, Disabled	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
review ↗			

1451.05iCSPOrganizational.2-05.i 05.02 External Parties

ID: 1451.05iCSPOrganizational.2-05.i Ownership: Shared

[\[\]](#) Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Assess risk in third party relationships ↗	CMA_0014 - Assess risk in third party relationships	Manual, Disabled	1.1.0 ↗
Audit privileged functions ↗	CMA_0019 - Audit privileged functions	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 ↗
Conduct a full text analysis of logged privileged commands ↗	CMA_0056 - Conduct a full text analysis of logged privileged commands	Manual, Disabled	1.1.0 ↗
Define access authorizations to support separation of duties ↗	CMA_0116 - Define access authorizations to support separation of duties	Manual, Disabled	1.1.0 ↗
Define and document government oversight ↗	CMA_C1587 - Define and document government oversight	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 ↗
Document separation of duties ↗	CMA_0204 - Document separation of duties	Manual, Disabled	1.1.0 ↗

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	1.1.0 ↗
Enforce software execution privileges ↗	CMA_C1041 - Enforce software execution privileges	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 ↗
Monitor privileged role assignment ↗	CMA_0378 - Monitor privileged role assignment	Manual, Disabled	1.1.0 ↗
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 ↗
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 ↗
Revoke privileged roles as appropriate ↗	CMA_0483 - Revoke privileged roles as appropriate	Manual, Disabled	1.1.0 ↗
Separate duties of individuals ↗	CMA_0492 - Separate duties of individuals	Manual, Disabled	1.1.0 ↗
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	1.1.0 ↗
Use privileged identity management ↗	CMA_0533 - Use privileged identity management	Manual, Disabled	1.1.0 ↗

1452.05kCSPOrganizational.1-05.k 05.02 External Parties

ID: 1452.05kCSPOrganizational.1-05.k 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	1.1.0 ↗
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	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 ↗

1453.05kCSPOrganizational.2-05.k 05.02 External Parties

ID: 1453.05kCSPOrganizational.2-05.k 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 ↗
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 ↗
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 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	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 ↗
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	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 ↗

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	1.1.0 ↗
Undergo independent security review ↗	CMA_0515 - Undergo independent security review	Manual, Disabled	1.1.0 ↗

1454.05kCSPOrganizational.3-05.k 05.02 External Parties

ID: 1454.05kCSPOrganizational.3-05.k 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 ↗
Define and document government oversight ↗	CMA_C1587 - Define and document government oversight	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 ↗
Establish policies for supply chain risk management ↗	CMA_0275 - Establish policies for supply chain risk management	Manual, Disabled	1.1.0 ↗
Identify external service providers ↗	CMA_C1591 - Identify external service providers	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 ↗

1455.05kCSPOrganizational.4-05.k 05.02 External Parties

ID: 1455.05kCSPOrganizational.4-05.k 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 ↗
Document third-party personnel security requirements ↗	CMA_C1531 - Document third-party personnel security requirements	Manual, Disabled	1.1.0 ↗
Establish third-party personnel security requirements ↗	CMA_C1529 - Establish third-party personnel security requirements	Manual, Disabled	1.1.0 ↗
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	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 ↗
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 ↗

1464.09e2Organizational.5-09.e 09.02 Control Third Party Service Delivery

ID: 1464.09e2Organizational.5-09.e 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 ↗

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

15 Incident Management

1501.02f1Organizational.123-02.f 02.03 During Employment

ID: 1501.02f1Organizational.123-02.f 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 ↗
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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement formal sanctions process ↗	CMA_0317 - Implement formal sanctions process	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 ↗
Notify personnel upon sanctions ↗	CMA_0380 - Notify personnel upon sanctions	Manual, Disabled	1.1.0 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

1503.02f2Organizational.12-02.f 02.03 During Employment

ID: 1503.02f2Organizational.12-02.f 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 ↗
Develop security safeguards ↗	CMA_0161 - Develop security safeguards	Manual, Disabled	1.1.0 ↗
Document security operations ↗	CMA_0202 - Document security operations	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 formal sanctions process ↗	CMA_0317 - Implement formal sanctions process	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 ↗
Implement Incident handling capability ↗	CMA_C1367 - Implement Incident handling capability	Manual, Disabled	1.1.0 ↗
Notify personnel upon sanctions ↗	CMA_0380 - Notify personnel upon sanctions	Manual, Disabled	1.1.0 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

1504.06e1Organizational.34-06.e 06.01 Compliance with Legal Requirements

ID: 1504.06e1Organizational.34-06.e 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 ↗
Create a data inventory ↗	CMA_0096 - Create a data inventory	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Document security operations ↗	CMA_0202 - Document security operations	Manual, Disabled	1.1.0 ↗
Enable detection of network devices ↗	CMA_0220 - Enable detection of network devices	Manual, Disabled	1.1.0 ↗
Enable network protection ↗	CMA_0238 - Enable network protection	Manual, Disabled	1.1.0 ↗
Enforce logical access ↗	CMA_0245 - Enforce logical access	Manual, Disabled	1.1.0 ↗

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 ↗
Implement formal sanctions process ↗	CMA_0317 - Implement formal sanctions process	Manual, Disabled	1.1.0 ↗
Implement incident handling ↗	CMA_0318 - Implement incident handling	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 ↗
Notify personnel upon sanctions ↗	CMA_0380 - Notify personnel upon sanctions	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 ↗
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 ↗

1505.11a1Organizational.13-11.a 11.01 Reporting Information Security Incidents and Weaknesses

ID: 1505.11a1Organizational.13-11.a 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 ↗
Conduct incident response testing ↗	CMA_0060 - Conduct incident response testing	Manual, Disabled	1.1.0 ↗
Develop an incident response	CMA_0145 - Develop an incident	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
plan ↗	response plan	Disabled	
Develop security safeguards ↗	CMA_0161 - Develop security safeguards	Manual, Disabled	1.1.0 ↗
Document security operations ↗	CMA_0202 - Document security operations	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 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	Manual, Disabled	1.1.0 ↗
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 ↗
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	1.1.0 ↗
Identify classes of Incidents and Actions taken ↗	CMA_C1365 - Identify classes of Incidents and Actions taken	Manual, Disabled	1.1.0 ↗
Identify incident response personnel ↗	CMA_0301 - Identify incident response personnel	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 ↗
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗
View and investigate restricted data ↗	CMA_0545 - View and investigate	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
users ↗	restricted users	Disabled	

1506.11a1Organizational.2-11.a 11.01 Reporting Information Security Incidents and Weaknesses

ID: 1506.11a1Organizational.2-11.a 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 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Document security operations ↗	CMA_0202 - Document security operations	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 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	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 ↗
Manage contacts for authorities and special interest groups ↗	CMA_0359 - Manage contacts for authorities and special interest groups	Manual, Disabled	1.1.0 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

1507.11a1Organizational.4-11.a 11.01 Reporting Information Security Incidents and Weaknesses

ID: 1507.11a1Organizational.4-11.a Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement an insider threat program ↗	CMA_C1751 - Implement an insider threat program	Manual, Disabled	1.1.0 ↗
Implement Incident handling capability ↗	CMA_C1367 - Implement Incident handling capability	Manual, Disabled	1.1.0 ↗
Provide security awareness training for insider threats ↗	CMA_0417 - Provide security awareness training for insider threats	Manual, Disabled	1.1.0 ↗

1508.11a2Organizational.1-11.a 11.01 Reporting Information Security Incidents and Weaknesses

ID: 1508.11a2Organizational.1-11.a 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 ↗
Document security operations ↗	CMA_0202 - Document security operations	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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

1509.11a2Organizational.236-11.a 11.01 Reporting Information Security Incidents and Weaknesses

ID: 1509.11a2Organizational.236-11.a 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 ↗
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 ↗
Document security operations ↗	CMA_0202 - Document security operations	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 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	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 classes of Incidents and Actions taken ↗	CMA_C1365 - Identify classes of Incidents and Actions taken	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 ↗
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

1510.11a2Organizational.47-11.a 11.01 Reporting Information Security Incidents and Weaknesses

ID: 1510.11a2Organizational.47-11.a 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 ↗
Conduct incident response testing ↗	CMA_0060 - Conduct incident response testing	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Document security operations ↗	CMA_0202 - Document security operations	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)
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 ↗
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗

1511.11a2Organizational.5-11.a 11.01 Reporting Information Security Incidents and Weaknesses

ID: 1511.11a2Organizational.5-11.a 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 safeguards	Manual, Disabled	1.1.0 ↗
Document security operations ↗	CMA_0202 - Document security operations	Manual, Disabled	1.1.0 ↗
Enable network protection ↗	CMA_0238 - Enable network protection	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Incorporate simulated events into incident response training ↗	CMA_C1356 - Incorporate simulated events into incident response training	Manual, Disabled	1.1.0 ↗
Maintain incident response plan ↗	CMA_0352 - Maintain incident response plan	Manual, Disabled	1.1.0 ↗
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

1512.11a2Organizational.8-11.a 11.01 Reporting Information Security Incidents and Weaknesses

ID: 1512.11a2Organizational.8-11.a 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 ↗
Correlate audit records ↗	CMA_0087 - Correlate audit records	Manual, Disabled	1.1.0 ↗
Develop an incident response plan ↗	CMA_0145 - Develop an incident response plan	Manual, Disabled	1.1.0 ↗
Document security operations ↗	CMA_0202 - Document security operations	Manual, Disabled	1.1.0 ↗
Document wireless access security controls ↗	CMA_C1695 - Document wireless access security controls	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 activity	Manual, Disabled	1.1.0 ↗
Review role group changes weekly ↗	CMA_0476 - Review role group changes weekly	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 ↗
Turn on sensors for endpoint security solution ↗	CMA_0514 - Turn on sensors for endpoint security solution	Manual, Disabled	1.1.0 ↗

1515.11a3Organizational.3-11.a 11.01 Reporting Information Security Incidents and Weaknesses

ID: 1515.11a3Organizational.3-11.a 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 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 ↗
Identify classes of Incidents and Actions taken ↗	CMA_C1365 - Identify classes of Incidents and Actions taken	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 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

1516.11c1Organizational.12-11.c 11.02 Management of Information Security Incidents and Improvements

ID: 1516.11c1Organizational.12-11.c 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct incident response testing ↗	CMA_0060 - Conduct incident response testing	Manual, Disabled	1.1.0 ↗
Document security operations ↗	CMA_0202 - Document security operations	Manual, Disabled	1.1.0 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	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 ↗
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗

1517.11c1Organizational.3-11.c 11.02 Management of Information Security Incidents and Improvements

ID: 1517.11c1Organizational.3-11.c 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 ↗
Document security operations ↗	CMA_0202 - Document security operations	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 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 ↗

1518.11c2Organizational.13-11.c 11.02 Management of Information Security Incidents and Improvements

ID: 1518.11c2Organizational.13-11.c 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 ↗

1519.11c2Organizational.2-11.c 11.02 Management of Information Security Incidents and Improvements

ID: 1519.11c2Organizational.2-11.c 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Integrate Audit record analysis ↗	CMA_C1120 - Integrate Audit record analysis	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 ↗
Provide capability to process customer-controlled audit records ↗	CMA_C1126 - Provide capability to process customer-controlled audit records	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 activity	Manual, Disabled	1.1.0 ↗
Review role group changes weekly ↗	CMA_0476 - Review role group changes weekly	Manual, Disabled	1.1.0 ↗

1520.11c2Organizational.4-11.c 11.02 Management of Information Security Incidents and Improvements

ID: 1520.11c2Organizational.4-11.c 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 ↗

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 ↗
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 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗

1521.11c2Organizational.56-11.c 11.02 Management of Information Security Incidents and Improvements

ID: 1521.11c2Organizational.56-11.c 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 ↗
Conduct incident response testing ↗	CMA_0060 - Conduct incident response testing	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 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Eradicate contaminated information ↗	CMA_0253 - Eradicate contaminated information	Manual, Disabled	1.1.0 ↗
Establish an information security program ↗	CMA_0263 - Establish an information security program	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 classes of Incidents and Actions taken ↗	CMA_C1365 - Identify classes of Incidents and Actions taken	Manual, Disabled	1.1.0 ↗
Implement incident handling ↗	CMA_0318 - Implement incident handling	Manual, Disabled	1.1.0 ↗
Implement Incident handling capability ↗	CMA_C1367 - Implement Incident handling capability	Manual, Disabled	1.1.0 ↗
Incorporate simulated events into incident response training ↗	CMA_C1356 - Incorporate simulated events into incident response training	Manual, Disabled	1.1.0 ↗
Maintain incident response plan ↗	CMA_0352 - Maintain incident response plan	Manual, Disabled	1.1.0 ↗
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

1522.11c3Organizational.13-11.c 11.02 Management of Information Security Incidents and Improvements

ID: 1522.11c3Organizational.13-11.c 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 ↗

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 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

1523.11c3Organizational.24-11.c 11.02 Management of Information Security Incidents and Improvements

ID: 1523.11c3Organizational.24-11.c 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 ↗
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 ↗
Use automated mechanisms for security alerts ↗	CMA_C1707 - Use automated mechanisms for security alerts	Manual, Disabled	1.1.0 ↗

1524.11a1Organizational.5-11.a 11.01 Reporting Information Security Incidents and Weaknesses

ID: 1524.11a1Organizational.5-11.a 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 ↗
Obtain legal opinion for monitoring system activities ↗	CMA_C1688 - Obtain legal opinion for monitoring system activities	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 ↗

1525.11a1Organizational.6-11.a 11.01 Reporting Information Security Incidents and Weaknesses

ID: 1525.11a1Organizational.6-11.a Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Establish information security workforce development and improvement program ↗	CMA_C1752 - Establish information security workforce development and improvement program	Manual, Disabled	1.1.0 ↗
Implement an insider threat program ↗	CMA_C1751 - Implement an insider threat program	Manual, Disabled	1.1.0 ↗
Implement formal sanctions process ↗	CMA_0317 - Implement formal sanctions process	Manual, Disabled	1.1.0 ↗
Implement Incident handling capability ↗	CMA_C1367 - Implement Incident handling capability	Manual, Disabled	1.1.0 ↗
Notify personnel upon sanctions ↗	CMA_0380 - Notify personnel upon sanctions	Manual, Disabled	1.1.0 ↗
Provide security awareness training for insider threats ↗	CMA_0417 - Provide security awareness training for insider threats	Manual, Disabled	1.1.0 ↗

1560.11d1Organizational.1-11.d 11.02 Management of Information Security Incidents and Improvements

ID: 1560.11d1Organizational.1-11.d 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 ↗
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 ↗
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 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗

1561.11d2Organizational.14-11.d 11.02 Management of Information Security Incidents and Improvements

ID: 1561.11d2Organizational.14-11.d 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 ↗
Enable network protection ↗	CMA_0238 - Enable network protection	Manual, Disabled	1.1.0 ↗
Eradicate contaminated	CMA_0253 - Eradicate contaminated	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
information ↗	information	Disabled	
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	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 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

1562.11d2Organizational.2-11.d 11.02 Management of Information Security Incidents and Improvements

ID: 1562.11d2Organizational.2-11.d Ownership: Shared

[+] Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Address information security issues ↗	CMA_C1742 - Address information security issues	Manual, Disabled	1.1.0 ↗
Conduct incident response testing ↗	CMA_0060 - Conduct incident response testing	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 contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0 ↗
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 ↗
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)
Execute actions in response to information spills ↗	CMA_0281 - Execute actions in response to information spills	Manual, Disabled	1.1.0 ↗
Identify classes of Incidents and Actions taken ↗	CMA_C1365 - Identify classes of Incidents and Actions taken	Manual, Disabled	1.1.0 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗
View and investigate restricted users ↗	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↗

1563.11d2Organizational.3-11.d 11.02 Management of Information Security Incidents and Improvements

ID: 1563.11d2Organizational.3-11.d 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 ↗
Conduct incident response testing ↗	CMA_0060 - Conduct incident response testing	Manual, Disabled	1.1.0 ↗
Maintain incident response plan ↗	CMA_0352 - Maintain incident response plan	Manual, Disabled	1.1.0 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗

1577.11aCSPOrganizational.1-11.a 11.01 Reporting Information Security Incidents and Weaknesses

ID: 1577.11aCSPOrganizational.1-11.a 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 ↴
Identify incident response personnel ↴	CMA_0301 - Identify incident response personnel	Manual, Disabled	1.1.0 ↴

1587.11c2Organizational.10-11.c 11.02 Management of Information Security Incidents and Improvements

ID: 1587.11c2Organizational.10-11.c 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 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 ↴
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 ↴
View and investigate restricted users ↴	CMA_0545 - View and investigate restricted users	Manual, Disabled	1.1.0 ↴

1589.11c1Organizational.5-11.c 11.02 Management of Information Security Incidents and Improvements

ID: 1589.11c1Organizational.5-11.c 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 ↗
Incorporate simulated events into incident response training ↗	CMA_C1356 - Incorporate simulated events into incident response training	Manual, Disabled	1.1.0 ↗
Provide information spillage training ↗	CMA_0413 - Provide information spillage training	Manual, Disabled	1.1.0 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗

16 Business Continuity & Disaster Recovery

1601.12c1Organizational.1238-12.c 12.01 Information Security Aspects of Business Continuity Management

ID: 1601.12c1Organizational.1238-12.c Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	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 ↗
Update contingency plan ↗	CMA_C1248 - Update contingency plan	Manual, Disabled	1.1.0 ↗

1602.12c1Organizational.4567-12.c 12.01 Information Security Aspects of Business Continuity Management

ID: 1602.12c1Organizational.4567-12.c 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 ↗
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 ↗

1603.12c1Organizational.9-12.c 12.01 Information Security Aspects of Business Continuity Management

ID: 1603.12c1Organizational.9-12.c 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 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 and update contingency planning policies and procedures ↗	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	1.1.0 ↗

1604.12c2Organizational.16789-12.c 12.01 Information Security Aspects of Business Continuity Management

ID: 1604.12c2Organizational.16789-12.c 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 ↗
Establish alternate storage site that facilitates recovery operations ↗	CMA_C1270 - Establish alternate storage site that facilitates recovery operations	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 ↗
Establish requirements for internet service providers ↗	CMA_0278 - Establish requirements for internet service providers	Manual, Disabled	1.1.0 ↗

1607.12c2Organizational.4-12.c 12.01 Information Security Aspects of Business Continuity Management

ID: 1607.12c2Organizational.4-12.c Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	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 ↗

1608.12c2Organizational.5-12.c 12.01 Information Security Aspects of Business Continuity Management

ID: 1608.12c2Organizational.5-12.c Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct backup of information system documentation ↗	CMA_C1289 - Conduct backup of information system documentation	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 ↗

1609.12c3Organizational.12-12.c 12.01 Information Security Aspects of Business Continuity Management

ID: 1609.12c3Organizational.12-12.c 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 ↗

1616.09I1Organizational.16-09.I 09.05 Information Back-Up

ID: 1616.09I1Organizational.16-09.I Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct backup of information system documentation ↗	CMA_C1289 - Conduct backup of information system documentation	Manual, Disabled	1.1.0 ↗
Long-term geo-redundant backup should be enabled for Azure SQL Databases ↗	This policy audits any Azure SQL Database with long-term geo-redundant backup not enabled.	AuditIfNotExists, Disabled	2.0.0 ↗

1617.09I1Organizational.23-09.I 09.05 Information Back-Up

ID: 1617.09I1Organizational.23-09.I Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct backup of information system documentation ↗	CMA_C1289 - Conduct backup of information system documentation	Manual, Disabled	1.1.0 ↗
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0 ↗
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 ↗

1618.09I1Organizational.45-09.I 09.05 Information Back-Up

ID: 1618.09I1Organizational.45-09.I Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version
(GitHub)		(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 ↗
Establish alternate storage site that facilitates recovery operations ↗	CMA_C1270 - Establish alternate storage site that facilitates recovery operations	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 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 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	1.0.1 ↗
Separately store backup information ↗	CMA_C1293 - Separately store backup information	Manual, Disabled	1.1.0 ↗

1619.09I1Organizational.7-09.I 09.05 Information Back-Up

ID: 1619.09I1Organizational.7-09.I 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 ↗
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 ↗

1620.09I1Organizational.8-09.I 09.05 Information Back-Up

ID: 1620.09I1Organizational.8-09.I 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 ↗
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 ↗

1621.09I2Organizational.1-09.I 09.05 Information Back-Up

ID: 1621.09I2Organizational.1-09.I Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Create a data inventory	CMA_0096 - Create a data inventory	Manual, Disabled	1.1.0
Long-term geo-redundant backup should be enabled for Azure SQL Databases	This policy audits any Azure SQL Database with long-term geo-redundant backup not enabled.	AuditIfNotExists, Disabled	2.0.0
Maintain records of processing of personal data	CMA_0353 - Maintain records of processing of personal data	Manual, Disabled	1.1.0

1622.09I2Organizational.23-09.I 09.05 Information Back-Up

ID: 1622.09I2Organizational.23-09.I 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
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
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
Separately store	CMA_C1293 - Separately store backup information	Manual,	1.1.0

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
backup information ↗		Disabled	

1623.09I2Organizational.4-09.I 09.05 Information Back-Up

ID: 1623.09I2Organizational.4-09.I Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
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 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	1.0.1 ↗

1624.09I3Organizational.12-09.I 09.05 Information Back-Up

ID: 1624.09I3Organizational.12-09.I Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Conduct backup of information system documentation ↗	CMA_C1289 - Conduct backup of information system documentation	Manual, Disabled	1.1.0 ↗

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

1625.09I3Organizational.34-09.I 09.05 Information Back-Up

ID: 1625.09I3Organizational.34-09.I Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)		(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 ↴

1626.09I3Organizational.5-09.I 09.05 Information Back-Up

ID: 1626.09I3Organizational.5-09.I Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct backup of information system documentation ↴	CMA_C1289 - Conduct backup of information system documentation	Manual, Disabled	1.1.0 ↴
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	1.0.1 ↴

1627.09I3Organizational.6-09.I 09.05 Information Back-Up

ID: 1627.09I3Organizational.6-09.I Ownership: Shared

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

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

1634.12b1Organizational.1-12.b 12.01 Information Security Aspects of Business Continuity Management

ID: 1634.12b1Organizational.1-12.b 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 https://aka.ms/asr-doc ↗.	auditIfNotExists	1.0.0 ↗
Coordinate contingency plans with related plans ↗	CMA_0086 - Coordinate contingency plans with related plans	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 ↗

1635.12b1Organizational.2-12.b 12.01 Information Security Aspects of Business Continuity Management

ID: 1635.12b1Organizational.2-12.b Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Key Vault Managed HSM should have purge protection enabled ↗	Malicious deletion of an Azure Key Vault Managed HSM can lead to permanent data loss. A malicious insider in your organization can potentially delete and purge Azure Key Vault Managed HSM. Purge protection protects you from insider attacks by enforcing a mandatory retention period for soft deleted Azure Key Vault Managed HSM. No one inside your organization or Microsoft will be able to purge your Azure Key Vault Managed HSM during the soft delete retention period.	Audit, Deny, Disabled	1.0.0 ↗
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0 ↗
Key vaults should have deletion	Malicious deletion of a key vault can lead to permanent data loss. You can prevent permanent	Audit, Deny,	2.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
protection enabled ↗	<p>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.</p> <p>Keep in mind that key vaults created after September 1st 2019 have soft-delete enabled by default.</p>	Disabled	
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 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	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 ↗

1636.12b2Organizational.1-12.b 12.01 Information Security Aspects of Business Continuity Management

ID: 1636.12b2Organizational.1-12.b 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 ↗
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0 ↗
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 ↗

1637.12b2Organizational.2-12.b 12.01 Information Security Aspects of Business Continuity Management

ID: 1637.12b2Organizational.2-12.b 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 ↗
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	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 ↗
Update contingency plan ↗	CMA_C1248 - Update contingency plan	Manual, Disabled	1.1.0 ↗
Windows machines should meet requirements for 'Security Options - Recovery console' ↗	Windows machines should have the specified Group Policy settings in the category 'Security Options - Recovery console' for allowing floppy copy and access to all drives and folders. This policy requires that the Guest Configuration prerequisites have been deployed to the policy assignment scope. For details, visit https://aka.ms/gcpol ↗.	AuditIfNotExists, Disabled	3.0.0 ↗

1638.12b2Organizational.345-12.b 12.01 Information Security Aspects of Business Continuity Management

ID: 1638.12b2Organizational.345-12.b 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 https://aka.ms/asr-doc .	auditIfNotExists	1.0.0
Conduct capacity planning	CMA_C1252 - Conduct capacity planning	Manual, Disabled	1.1.0
Develop contingency plan	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0
Perform a risk assessment	CMA_0388 - Perform a risk assessment	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

1666.12d1Organizational.1235-12.d 12.01 Information Security Aspects of Business Continuity Management

ID: 1666.12d1Organizational.1235-12.d 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 contingency plan	CMA_C1244 - Develop contingency plan	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

1667.12d1Organizational.4-12.d 12.01 Information Security Aspects of Business Continuity Management

ID: 1667.12d1Organizational.4-12.d 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 ↗
Update contingency plan ↗	CMA_C1248 - Update contingency plan	Manual, Disabled	1.1.0 ↗

1668.12d1Organizational.67-12.d 12.01 Information Security Aspects of Business Continuity Management

ID: 1668.12d1Organizational.67-12.d Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	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 ↗
Review and update contingency planning policies and procedures ↗	CMA_C1243 - Review and update contingency planning policies and procedures	Manual, Disabled	1.1.0 ↗

1669.12d1Organizational.8-12.d 12.01 Information Security Aspects of Business Continuity Management

ID: 1669.12d1Organizational.8-12.d Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0 ↗
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 ↗
Plan for resumption of essential business functions ↗	CMA_C1253 - Plan for resumption of essential business functions	Manual, Disabled	1.1.0 ↗
Provide contingency training ↗	CMA_0412 - Provide contingency training	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 ↗
Update contingency plan ↗	CMA_C1248 - Update contingency plan	Manual, Disabled	1.1.0 ↗

1670.12d2Organizational.1-12.d 12.01 Information Security Aspects of Business Continuity Management

ID: 1670.12d2Organizational.1-12.d Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Develop contingency plan ↗	CMA_C1244 - Develop contingency plan	Manual, Disabled	1.1.0 ↗

1671.12d2Organizational.2-12.d 12.01 Information Security Aspects of Business Continuity Management

ID: 1671.12d2Organizational.2-12.d 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 ↗
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 ↗

1672.12d2Organizational.3-12.d 12.01 Information Security Aspects of Business Continuity Management

ID: 1672.12d2Organizational.3-12.d 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 contingency plan ↗	CMA_C1244 - Develop contingency plan	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 ↗
Update contingency plan ↗	CMA_C1248 - Update contingency plan	Manual, Disabled	1.1.0 ↗

17 Risk Management

1704.03b1Organizational.12-03.b 03.01 Risk Management Program

ID: 1704.03b1Organizational.12-03.b 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 ↗
Perform a risk assessment ↗	CMA_0388 - Perform a risk assessment	Manual, Disabled	1.1.0 ↗

1705.03b2Organizational.12-03.b 03.01 Risk Management Program

ID: 1705.03b2Organizational.12-03.b 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 ↗

1707.03c1Organizational.12-03.c 03.01 Risk Management Program

ID: 1707.03c1Organizational.12-03.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 ↗

1708.03c2Organizational.12-03.c 03.01 Risk Management Program

ID: 1708.03c2Organizational.12-03.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 ↗
Update POA&M items ↗	CMA_C1157 - Update POA&M items	Manual, Disabled	1.1.0 ↗

17100.10a3Organizational.5 10.01 Security Requirements of Information Systems

ID: 17100.10a3Organizational.5 Ownership: Shared

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

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

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 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 ↗

17101.10a3Organizational.6-10.a 10.01 Security Requirements of Information Systems

ID: 17101.10a3Organizational.6-10.a Ownership: Shared

C 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 ↗
Establish a secure software development program ↗	CMA_0259 - Establish a secure software development program	Manual, Disabled	1.1.0 ↗
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 ↗
Obtain functional properties of security controls ↗	CMA_C1575 - Obtain functional properties of security controls	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 ↗

17120.10a3Organizational.5-10.a 10.01 Security Requirements of Information Systems

ID: 17120.10a3Organizational.5-10.a 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 ↗
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 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 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 ↗
Obtain approvals for acquisitions and outsourcing ↗	CMA_C1590 - Obtain approvals for acquisitions and outsourcing	Manual, Disabled	1.1.0 ↗

17126.03c1System.6-03.c 03.01 Risk Management Program

ID: 17126.03c1System.6-03.c Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct risk assessment and document its results ↗	CMA_C1542 - Conduct risk assessment and document its results	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 ↗

1713.03c1Organizational.3-03.c 03.01 Risk Management Program

ID: 1713.03c1Organizational.3-03.c Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define the duties of processors ↗	CMA_0127 - Define the duties of processors	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 ↗
Evaluate and review PII holdings regularly ↗	CMA_C1832 - Evaluate and review PII holdings regularly	Manual, Disabled	1.1.0 ↗
Issue guidelines for ensuring data quality and integrity ↗	CMA_C1824 - Issue guidelines for ensuring data quality and integrity	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 ↗
Perform disposition review ↗	CMA_0391 - Perform disposition review	Manual, Disabled	1.1.0 ↗
Record disclosures of PII to third parties ↗	CMA_0422 - Record disclosures of PII to third parties	Manual, Disabled	1.1.0 ↗
Train staff on PII sharing and its consequences ↗	CMA_C1871 - Train staff on PII sharing and its consequences	Manual, Disabled	1.1.0 ↗

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

1733.03d1Organizational.1-03.d 03.01 Risk Management Program

ID: 1733.03d1Organizational.1-03.d 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 document its results ↗	CMA_C1542 - Conduct risk assessment and document its results	Manual, Disabled	1.1.0 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗

1734.03d2Organizational.1-03.d 03.01 Risk Management Program

ID: 1734.03d2Organizational.1-03.d 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 ↗

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 ↗
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 ↗

1735.03d2Organizational.23-03.d 03.01 Risk Management Program

ID: 1735.03d2Organizational.23-03.d 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 ↗
Conduct risk assessment and distribute its results ↗	CMA_C1544 - Conduct risk assessment and distribute its results	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 configuration management requirements for developers ↗	CMA_0270 - Establish configuration management requirements for developers	Manual, Disabled	1.1.0 ↗
Integrate risk management process into SDLC ↗	CMA_C1567 - Integrate risk management process into SDLC	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	1.1.0 ↗
Perform audit for configuration change control ↗	CMA_0390 - Perform audit for configuration change control	Manual, Disabled	1.1.0 ↗

1736.03d2Organizational.4-03.d 03.01 Risk Management Program

ID: 1736.03d2Organizational.4-03.d Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Conduct risk assessment and document its results ↗	CMA_C1542 - Conduct risk assessment and document its results	Manual, Disabled	1.1.0 ↗

1737.03d2Organizational.5-03.d 03.01 Risk Management Program

ID: 1737.03d2Organizational.5-03.d 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 ↗
Establish a risk management strategy ↗	CMA_0258 - Establish a risk management strategy	Manual, Disabled	1.1.0 ↗

1780.10a1Organizational.1-10.a 10.01 Security Requirements of Information Systems

ID: 1780.10a1Organizational.1-10.a 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 ↗
Develop access control policies and procedures ↗	CMA_0144 - Develop access control policies and procedures	Manual, Disabled	1.1.0 ↗
Govern policies and procedures ↗	CMA_0292 - Govern policies and procedures	Manual, Disabled	1.1.0 ↗

1781.10a1Organizational.23-10.a 10.01 Security Requirements of Information Systems

ID: 1781.10a1Organizational.23-10.a 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 ↗
Develop a concept of operations (CONOPS) ↗	CMA_0141 - Develop a concept of operations (CONOPS)	Manual, Disabled	1.1.0 ↗
Develop SSP that meets criteria ↗	CMA_C1492 - Develop SSP that meets criteria	Manual, Disabled	1.1.0 ↗
Integrate risk management process into SDLC ↗	CMA_C1567 - Integrate risk management process into SDLC	Manual, Disabled	1.1.0 ↗

1782.10a1Organizational.4-10.a 10.01 Security Requirements of Information Systems

ID: 1782.10a1Organizational.4-10.a 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 ↗

1783.10a1Organizational.56-10.a 10.01 Security Requirements of Information Systems

ID: 1783.10a1Organizational.56-10.a Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 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	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	data in contracts		
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 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 ↗

1784.10a1Organizational.7-10.a 10.01 Security Requirements of Information Systems

ID: 1784.10a1Organizational.7-10.a Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Employ FIPS 201-approved technology for PIV ↗	CMA_C1579 - Employ FIPS 201-approved technology for PIV	Manual, Disabled	1.1.0 ↗

1785.10a1Organizational.8-10.a 10.01 Security Requirements of Information Systems

ID: 1785.10a1Organizational.8-10.a 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Create alternative actions for identified anomalies ↗	CMA_C1711 - Create alternative actions for identified anomalies	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 ↗
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 ↗

1786.10a1Organizational.9-10.a 10.01 Security Requirements of Information Systems

ID: 1786.10a1Organizational.9-10.a 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 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 ↗
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 ↗

1787.10a2Organizational.1-10.a 10.01 Security Requirements of Information Systems

ID: 1787.10a2Organizational.1-10.a Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate privacy controls ↗	CMA_C1817 - Automate privacy controls	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 a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗
Information security and personal data protection ↗	CMA_0332 - Information security and personal data protection	Manual, Disabled	1.1.0 ↗
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	1.1.0 ↗

1788.10a2Organizational.2-10.a 10.01 Security Requirements of Information Systems

ID: 1788.10a2Organizational.2-10.a 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 ↗
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 ↗
Establish a secure software development program ↗	CMA_0259 - Establish a secure software development program	Manual, Disabled	1.1.0 ↗
Perform a privacy impact assessment ↗	CMA_0387 - Perform a privacy impact assessment	Manual, Disabled	1.1.0 ↗

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

1789.10a2Organizational.3-10.a 10.01 Security Requirements of Information Systems

ID: 1789.10a2Organizational.3-10.a 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 ↗
Develop a concept of operations (CONOPS) ↗	CMA_0141 - Develop a concept of operations (CONOPS)	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 ↗

1790.10a2Organizational.45-10.a 10.01 Security Requirements of Information Systems

ID: 1790.10a2Organizational.45-10.a 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 ↗
Develop a concept of operations (CONOPS) ↗	CMA_0141 - Develop a concept of operations (CONOPS)	Manual, Disabled	1.1.0 ↗
Develop SSP that meets criteria ↗	CMA_C1492 - Develop SSP that meets criteria	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 ↗

1791.10a2Organizational.6-10.a 10.01 Security Requirements of Information Systems

ID: 1791.10a2Organizational.6-10.a Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate flaw remediation ↗	CMA_0027 - Automate flaw remediation	Manual, Disabled	1.1.0 ↗
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 ↗
Integrate risk management process into SDLC ↗	CMA_C1567 - Integrate risk management process into SDLC	Manual, Disabled	1.1.0 ↗
View and configure system diagnostic data ↗	CMA_0544 - View and configure system diagnostic data	Manual, Disabled	1.1.0 ↗

1792.10a2Organizational.7814-10.a 10.01 Security Requirements of Information Systems

ID: 1792.10a2Organizational.7814-10.a 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 ↗
Implement the risk management strategy ↗	CMA_C1744 - Implement the risk management strategy	Manual, Disabled	1.1.0 ↗
Integrate risk management process into SDLC ↗	CMA_C1567 - Integrate risk management process into SDLC	Manual, Disabled	1.1.0 ↗

1793.10a2Organizational.91011-10.a 10.01 Security Requirements of Information Systems

ID: 1793.10a2Organizational.91011-10.a 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	CMA_0279 - Establish security requirements for the manufacturing	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
connected devices ↗	of connected devices		
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗

1794.10a2Organizational.12-10.a 10.01 Security Requirements of Information Systems

ID: 1794.10a2Organizational.12-10.a Ownership: Shared

↔ Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require developers to produce evidence of security assessment plan execution ↗	CMA_C1602 - Require developers to produce evidence of security assessment plan execution	Manual, Disabled	1.1.0 ↗

1795.10a2Organizational.13-10.a 10.01 Security Requirements of Information Systems

ID: 1795.10a2Organizational.13-10.a 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 ↗
Establish a secure software development program ↗	CMA_0259 - Establish a secure software development program	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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Require developers to produce evidence of security assessment plan execution ↗	CMA_C1602 - Require developers to produce evidence of security assessment plan execution	Manual, Disabled	1.1.0 ↗

1796.10a2Organizational.15-10.a 10.01 Security Requirements of Information Systems

ID: 1796.10a2Organizational.15-10.a 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 ↗
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 ↗
Employ independent assessors to conduct security control assessments ↗	CMA_C1148 - Employ independent assessors to conduct security control assessments	Manual, Disabled	1.1.0 ↗
Produce Security Assessment report ↗	CMA_C1146 - Produce Security Assessment report	Manual, Disabled	1.1.0 ↗

1797.10a3Organizational.1-10.a 10.01 Security Requirements of Information Systems

ID: 1797.10a3Organizational.1-10.a 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	1.1.0 ↗
Develop an enterprise architecture ↗	CMA_C1741 - Develop an enterprise architecture	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 ↗

1798.10a3Organizational.2-10.a 10.01 Security Requirements of Information Systems

ID: 1798.10a3Organizational.2-10.a 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	1.1.0 ↗
Develop an enterprise architecture ↗	CMA_C1741 - Develop an enterprise architecture	Manual, Disabled	1.1.0 ↗
Require developers to build security architecture ↗	CMA_C1612 - Require developers to build security architecture	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 ↗

1799.10a3Organizational.34-10.a 10.01 Security Requirements of Information Systems

ID: 1799.10a3Organizational.34-10.a 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	1.1.0 ↗
Develop an enterprise architecture ↗	CMA_C1741 - Develop an enterprise architecture	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 and update the information security architecture ↗	CMA_C1504 - Review and update the information security architecture	Manual, Disabled	1.1.0 ↗

18 Physical & Environmental Security

1801.08b1Organizational.124-08.b 08.01 Secure Areas

ID: 1801.08b1Organizational.124-08.b 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 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 ↗
Monitor third-party provider compliance ↗	CMA_C1533 - Monitor third-party provider compliance	Manual, Disabled	1.1.0 ↗

1802.08b1Organizational.3-08.b 08.01 Secure Areas

ID: 1802.08b1Organizational.3-08.b Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Control physical access ↗	CMA_0081 - Control physical access	Manual, Disabled	1.1.0 ↗

1803.08b1Organizational.5-08.b 08.01 Secure Areas

ID: 1803.08b1Organizational.5-08.b Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(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 ↗
Produce complete records of remote maintenance activities ↗	CMA_C1403 - Produce complete records of remote maintenance activities	Manual, Disabled	1.1.0 ↗

1804.08b2Organizational.12-08.b 08.01 Secure Areas

ID: 1804.08b2Organizational.12-08.b Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Control physical access ↗	CMA_0081 - Control physical access	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 ↗

1805.08b2Organizational.3-08.b 08.01 Secure Areas

ID: 1805.08b2Organizational.3-08.b Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Control physical access ↗	CMA_0081 - Control physical access	Manual, Disabled	1.1.0 ↗

1806.08b2Organizational.4-08.b 08.01 Secure Areas

ID: 1806.08b2Organizational.4-08.b Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Control physical access ↗	CMA_0081 - Control physical access	Manual, Disabled	1.1.0 ↗

1807.08b2Organizational.56-08.b 08.01 Secure Areas

ID: 1807.08b2Organizational.56-08.b Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Control physical access ↗	CMA_0081 - Control physical access	Manual, Disabled	1.1.0 ↗

1808.08b2Organizational.7-08.b 08.01 Secure Areas

ID: 1808.08b2Organizational.7-08.b Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Audit user account status ↗	CMA_0020 - Audit user account	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	status	Disabled	
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 ↗
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 ↗
Review account provisioning logs ↗	CMA_0460 - Review account provisioning logs	Manual, Disabled	1.1.0 ↗
Review user accounts ↗	CMA_0480 - Review user accounts	Manual, Disabled	1.1.0 ↗
Separate duties of individuals ↗	CMA_0492 - Separate duties of individuals	Manual, Disabled	1.1.0 ↗

1810.08b3Organizational.2-08.b 08.01 Secure Areas

ID: 1810.08b3Organizational.2-08.b 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 ↗

18108.08j1Organizational.1-08.j 08.02 Equipment Security

ID: 18108.08j1Organizational.1-08.j 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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Review and update system maintenance policies and procedures ↗	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	1.1.0 ↗

18109.08j1Organizational.4-08.j 08.02 Equipment Security

ID: 18109.08j1Organizational.4-08.j 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 ↗
Employ a media sanitization mechanism ↗	CMA_0208 - Employ a media sanitization mechanism	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 ↗

1811.08b3Organizational.3-08.b 08.01 Secure Areas

ID: 1811.08b3Organizational.3-08.b 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 ↗
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 ↗

18110.08j1Organizational.5-08.j 08.02 Equipment Security

ID: 18110.08j1Organizational.5-08.j 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	1.1.0 ↗
Implement cryptographic mechanisms ↗	CMA_C1419 - Implement cryptographic mechanisms	Manual, Disabled	1.1.0 ↗
Manage nonlocal maintenance and diagnostic activities ↗	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	1.1.0 ↗
Perform all non-local maintenance ↗	CMA_C1417 - Perform all non-local maintenance	Manual, Disabled	1.1.0 ↗

18111.08j1Organizational.6-08.j 08.02 Equipment Security

ID: 18111.08j1Organizational.6-08.j 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 ↗

18112.08j3Organizational.4-08.j 08.02 Equipment Security

ID: 18112.08j3Organizational.4-08.j 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 ↗
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 system maintenance policies and procedures ↗	CMA_C1395 - Review and update system maintenance policies and procedures	Manual, Disabled	1.1.0 ↗

1812.08b3Organizational.46-08.b 08.01 Secure Areas

ID: 1812.08b3Organizational.46-08.b 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 ↗
Install an alarm system ↗	CMA_0338 - Install an alarm system	Manual, Disabled	1.1.0 ↗
Manage a secure surveillance camera system ↗	CMA_0354 - Manage a secure surveillance camera system	Manual, Disabled	1.1.0 ↗

18127.08I1Organizational.3-08.I 08.02 Equipment Security

ID: 18127.08I1Organizational.3-08.I 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 ↗

1813.08b3Organizational.56-08.b 08.01 Secure Areas

ID: 1813.08b3Organizational.56-08.b 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 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 ↗
Manage a secure surveillance camera system ↗	CMA_0354 - Manage a secure surveillance camera system	Manual, Disabled	1.1.0 ↗

18130.09p1Organizational.24-09.p 09.07 Media Handling

ID: 18130.09p1Organizational.24-09.p 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 ↗

1814.08d1Organizational.12-08.d 08.01 Secure Areas

ID: 1814.08d1Organizational.12-08.d Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement a penetration testing methodology ↗	CMA_0306 - Implement a penetration testing methodology	Manual, Disabled	1.1.0 ↗

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 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗

18145.08b3Organizational.7-08.b 08.01 Secure Areas

ID: 18145.08b3Organizational.7-08.b Ownership: Shared

↔ Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Install an alarm system ↗	CMA_0338 - Install an alarm system	Manual, Disabled	1.1.0 ↗
Manage a secure surveillance camera system ↗	CMA_0354 - Manage a secure surveillance camera system	Manual, Disabled	1.1.0 ↗

18146.08b3Organizational.8-08.b 08.01 Secure Areas

ID: 18146.08b3Organizational.8-08.b 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 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 ↗
Manage a secure surveillance camera system ↗	CMA_0354 - Manage a secure surveillance camera system	Manual, Disabled	1.1.0 ↗

1815.08d2Organizational.123-08.d 08.01 Secure Areas

ID: 1815.08d2Organizational.123-08.d Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
Implement a penetration testing methodology ↗	CMA_0306 - Implement a penetration testing methodology	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 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗

1816.08d2Organizational.4-08.d 08.01 Secure Areas

ID: 1816.08d2Organizational.4-08.d Ownership: Shared

[Expand table](#)

Name	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 ↗
Install an alarm system ↗	CMA_0338 - Install an alarm system	Manual, Disabled	1.1.0 ↗
Manage a secure surveillance camera system ↗	CMA_0354 - Manage a secure surveillance camera system	Manual, Disabled	1.1.0 ↗
Manage the transportation of assets ↗	CMA_0370 - Manage the transportation of assets	Manual, Disabled	1.1.0 ↗

1817.08d3Organizational.12-08.d 08.01 Secure Areas

ID: 1817.08d3Organizational.12-08.d 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 ↗

1818.08d3Organizational.3-08.d 08.01 Secure Areas

ID: 1818.08d3Organizational.3-08.d Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement a penetration testing methodology ↗	CMA_0306 - Implement a penetration testing methodology	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 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗

1819.08j1Organizational.23-08.j 08.02 Equipment Security

ID: 1819.08j1Organizational.23-08.j 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 ↗
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	Manual, Disabled	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal) Manage maintenance personnel ↗	CMA_C1421 - Manage maintenance personnel	Manual, Disabled	(GitHub) 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 ↗

1820.08j2Organizational.1-08.j 08.02 Equipment Security

ID: 1820.08j2Organizational.1-08.j Ownership: Shared

[\[\]](#) Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Control maintenance and repair activities ↗	CMA_0080 - Control maintenance and repair activities	Manual, Disabled	1.1.0 ↗
Manage nonlocal maintenance and diagnostic activities ↗	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	1.1.0 ↗

1821.08j2Organizational.3-08.j 08.02 Equipment Security

ID: 1821.08j2Organizational.3-08.j Ownership: Shared

[\[\]](#) Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(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 ↗
Manage nonlocal maintenance and diagnostic activities ↗	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Produce complete records of remote maintenance activities ↗	CMA_C1403 - Produce complete records of remote maintenance activities	Manual, Disabled	1.1.0 ↗

1822.08j2Organizational.2-08.j 08.02 Equipment Security

ID: 1822.08j2Organizational.2-08.j 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 ↗
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 ↗

1823.08j3Organizational.12-08.j 08.02 Equipment Security

ID: 1823.08j3Organizational.12-08.j 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	1.1.0 ↗
Manage nonlocal maintenance and diagnostic activities ↗	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	1.1.0 ↗

1824.08j3Organizational.3-08.j 08.02 Equipment Security

ID: 1824.08j3Organizational.3-08.j 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	1.1.0 ↗
Manage nonlocal maintenance and diagnostic activities	CMA_0364 - Manage nonlocal maintenance and diagnostic activities	Manual, Disabled	1.1.0 ↗

1826.09p1Organizational.1-09.p 09.07 Media Handling

ID: 1826.09p1Organizational.1-09.p 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 ↗
Perform disposition review	CMA_0391 - Perform disposition review	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 ↗

1844.08b1Organizational.6-08.b 08.01 Secure Areas

ID: 1844.08b1Organizational.6-08.b 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 ↗

1845.08b1Organizational.7-08.b 08.01 Secure Areas

ID: 1845.08b1Organizational.7-08.b 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 ↗
Define a physical key management process ↗	CMA_0115 - Define a physical key management process	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 ↗

1846.08b2Organizational.8-08.b 08.01 Secure Areas

ID: 1846.08b2Organizational.8-08.b 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 ↗

1847.08b2Organizational.910-08.b 08.01 Secure Areas

ID: 1847.08b2Organizational.910-08.b Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define a physical key	CMA_0115 - Define a physical key	Manual,	1.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
management process ↗	management process	Disabled	
Establish and maintain an asset inventory ↗	CMA_0266 - Establish and maintain an asset inventory	Manual, Disabled	1.1.0 ↗

1848.08b2Organizational.11-08.b 08.01 Secure Areas

ID: 1848.08b2Organizational.11-08.b 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 ↗

1862.08d1Organizational.3-08.d 08.01 Secure Areas

ID: 1862.08d1Organizational.3-08.d Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement a penetration testing methodology ↗	CMA_0306 - Implement a penetration testing methodology	Manual, Disabled	1.1.0 ↗
Run simulation attacks ↗	CMA_0486 - Run simulation attacks	Manual, Disabled	1.1.0 ↗

1862.08d3Organizational.3 08.01 Secure Areas

ID: 1862.08d3Organizational.3 Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement a penetration testing methodology ↗	CMA_0306 - Implement a penetration testing methodology	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 ↗

1892.01I1Organizational.1 01.04 Network Access Control

ID: 1892.01I1Organizational.1 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 ↗
Establish and maintain an asset inventory ↗	CMA_0266 - Establish and maintain an asset inventory	Manual, Disabled	1.1.0 ↗

19 Data Protection & Privacy

1901.06d1Organizational.1-06.d 06.01 Compliance with Legal Requirements

ID: 1901.06d1Organizational.1-06.d 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 ↗
Establish a privacy program ↗	CMA_0257 - Establish a privacy program	Manual, Disabled	1.1.0 ↗
Manage compliance activities ↗	CMA_0358 - Manage compliance	Manual,	1.1.0 ↗

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

1902.06d1Organizational.2-06.d 06.01 Compliance with Legal Requirements

ID: 1902.06d1Organizational.2-06.d Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define the duties of processors ↗	CMA_0127 - Define the duties of processors	Manual, Disabled	1.1.0 ↗
Document and distribute a privacy policy ↗	CMA_0188 - Document and distribute a privacy policy	Manual, Disabled	1.1.0 ↗
Implement privacy notice delivery methods ↗	CMA_0324 - Implement privacy notice delivery methods	Manual, Disabled	1.1.0 ↗
Keep accurate accounting of disclosures of information ↗	CMA_C1818 - Keep accurate accounting of disclosures of information	Manual, Disabled	1.1.0 ↗
Make accounting of disclosures available upon request ↗	CMA_C1820 - Make accounting of disclosures available upon request	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 ↗
Record disclosures of PII to third parties ↗	CMA_0422 - Record disclosures of PII to third parties	Manual, Disabled	1.1.0 ↗
Restrict communications ↗	CMA_0449 - Restrict communications	Manual, Disabled	1.1.0 ↗
Retain accounting of disclosures of information ↗	CMA_C1819 - Retain accounting of disclosures of information	Manual, Disabled	1.1.0 ↗
Train staff on PII sharing and its consequences ↗	CMA_C1871 - Train staff on PII sharing and its consequences	Manual, Disabled	1.1.0 ↗

1903.06d1Organizational.3456711-06.d 06.01 Compliance with Legal Requirements

ID: 1903.06d1Organizational.3456711-06.d Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Define cryptographic use ↗	CMA_0120 - Define cryptographic use	Manual, Disabled	1.1.0 ↗
Establish a data leakage management procedure ↗	CMA_0255 - Establish a data leakage management procedure	Manual, Disabled	1.1.0 ↗
Implement training for protecting authenticators ↗	CMA_0329 - Implement training for protecting authenticators	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 special information ↗	CMA_0409 - Protect special information	Manual, Disabled	1.1.0 ↗

1904.06.d2Organizational.1-06.d 06.01 Compliance with Legal Requirements

ID: 1904.06.d2Organizational.1-06.d 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 ↗
Perform disposition review ↗	CMA_0391 - Perform disposition review	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 ↗

1906.06.c1Organizational.2-06.c 06.01 Compliance with Legal Requirements

ID: 1906.06.c1Organizational.2-06.c Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Make SORNs available publicly ↗	CMA_C1865 - Make SORNs available publicly	Manual, Disabled	1.1.0 ↗
Provide formal notice to individuals ↗	CMA_C1864 - Provide formal notice to individuals	Manual, Disabled	1.1.0 ↗
Provide privacy notice to the public and to individuals ↗	CMA_C1861 - Provide privacy notice to the public and to individuals	Manual, Disabled	1.1.0 ↗
Publish SORNs for systems containing PII ↗	CMA_C1862 - Publish SORNs for systems containing PII	Manual, Disabled	1.1.0 ↗

1907.06.c1Organizational.3-06.c 06.01 Compliance with Legal Requirements

ID: 1907.06.c1Organizational.3-06.c Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Keep SORNs updated ↗	CMA_C1863 - Keep SORNs updated	Manual, Disabled	1.1.0 ↗
Make SORNs available publicly ↗	CMA_C1865 - Make SORNs available publicly	Manual, Disabled	1.1.0 ↗
Provide formal notice to individuals ↗	CMA_C1864 - Provide formal notice to individuals	Manual, Disabled	1.1.0 ↗
Publish SORNs for systems containing PII ↗	CMA_C1862 - Publish SORNs for systems containing PII	Manual, Disabled	1.1.0 ↗

1908.06.c1Organizational.4-06.c 06.01 Compliance with Legal Requirements

ID: 1908.06.c1Organizational.4-06.c 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
Establish backup policies and procedures	CMA_0268 - Establish backup policies and procedures	Manual, Disabled	1.1.0
Keep SORNs updated	CMA_C1863 - Keep SORNs updated	Manual, Disabled	1.1.0
Make SORNs available publicly	CMA_C1865 - Make SORNs available publicly	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
Provide formal notice to individuals	CMA_C1864 - Provide formal notice to individuals	Manual, Disabled	1.1.0
Publish SORNs for systems containing PII	CMA_C1862 - Publish SORNs for systems containing PII	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 label activity and analytics	CMA_0474 - Review label activity and analytics	Manual, Disabled	1.1.0

1911.06d1Organizational.13-06.d 06.01 Compliance with Legal Requirements

ID: 1911.06d1Organizational.13-06.d Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document the legal basis for processing personal information ↗	CMA_0206 - Document the legal basis for processing personal information	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 ↗
Evaluate and review PII holdings regularly ↗	CMA_C1832 - Evaluate and review PII holdings regularly	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 ↗
Remove or redact any PII ↗	CMA_C1833 - Remove or redact any PII	Manual, Disabled	1.1.0 ↗

19134.05j1Organizational.5-05.j 05.02 External Parties

ID: 19134.05j1Organizational.5-05.j 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 ↗
Designate authorized personnel to post publicly accessible information ↗	CMA_C1083 - Designate authorized personnel to post publicly accessible information	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 ↗
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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Implement security engineering principles of information systems ↗	CMA_0325 - Implement security engineering principles of information systems	Manual, Disabled	1.1.0 ↗
Information security and personal data protection ↗	CMA_0332 - Information security and personal data protection	Manual, Disabled	1.1.0 ↗
Manage compliance activities ↗	CMA_0358 - Manage compliance activities	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 information	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 ↗
Update privacy plan, policies, and procedures ↗	CMA_C1807 - Update privacy plan, policies, and procedures	Manual, Disabled	1.1.0 ↗

19141.06c1Organizational.7-06.c 06.01 Compliance with Legal Requirements

ID: 19141.06c1Organizational.7-06.c 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 ↗
Enforce logical access ↗	CMA_0245 - Enforce logical access	Manual, Disabled	1.1.0 ↗

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 ↗
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 ↗
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 ↗

19142.06c1Organizational.8-06.c 06.01 Compliance with Legal Requirements

ID: 19142.06c1Organizational.8-06.c 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 ↗
Control use of portable storage devices ↗	CMA_0083 - Control use of portable storage devices	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 ↗
Perform disposition review ↗	CMA_0391 - Perform disposition review	Manual, Disabled	1.1.0 ↗
Restrict media use ↗	CMA_0450 - Restrict media use	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	1.1.0 ↗
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	1.1.0 ↗
Review label activity and analytics ↗	CMA_0474 - Review label activity and analytics	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 ↗

19143.06c1Organizational.9-06.c 06.01 Compliance with Legal Requirements

ID: 19143.06c1Organizational.9-06.c 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 ↗
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 ↗
Develop SSP that meets criteria ↗	CMA_C1492 - Develop SSP that meets criteria	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 ↗

19144.06c2Organizational.1-06.c 06.01 Compliance with Legal Requirements

ID: 19144.06c2Organizational.1-06.c 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 ↗
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 ↗
Perform disposition review ↗	CMA_0391 - Perform disposition review	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 label activity and analytics ↗	CMA_0474 - Review label activity and analytics	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 ↗

19145.06c2Organizational.2-06.c 06.01 Compliance with Legal Requirements

ID: 19145.06c2Organizational.2-06.c 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 ↗
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 ↗
Perform disposition review ↗	CMA_0391 - Perform disposition review	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	1.1.0 ↗
Retain terminated user data ↗	CMA_0455 - Retain terminated user data	Manual, Disabled	1.1.0 ↗
Review label activity and analytics ↗	CMA_0474 - Review label activity and analytics	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 ↗

19242.06d1Organizational.14-06.d 06.01 Compliance with Legal Requirements

ID: 19242.06d1Organizational.14-06.d Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Document the legal basis for processing personal information ↗	CMA_0206 - Document the legal basis for processing personal information	Manual, Disabled	1.1.0 ↗
Evaluate and review PII holdings regularly ↗	CMA_C1832 - Evaluate and review PII holdings regularly	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 ↗
Remove or redact any PII ↗	CMA_C1833 - Remove or redact any PII	Manual, Disabled	1.1.0 ↗

19243.06d1Organizational.15-06.d 06.01 Compliance with Legal Requirements

ID: 19243.06d1Organizational.15-06.d Ownership: Shared

[\[\]](#) Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Automate privacy controls ↗	CMA_C1817 - Automate privacy controls	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 ↗
Evaluate and review PII holdings regularly ↗	CMA_C1832 - Evaluate and review PII holdings regularly	Manual, Disabled	1.1.0 ↗
Implement privacy notice delivery methods ↗	CMA_0324 - Implement privacy notice delivery methods	Manual, Disabled	1.1.0 ↗
Information security and personal data protection ↗	CMA_0332 - Information security and personal data protection	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 ↗
Remove or redact any PII ↗	CMA_C1833 - Remove or redact any PII	Manual, Disabled	1.1.0 ↗
Restrict communications ↗	CMA_0449 - Restrict communications	Manual, Disabled	1.1.0 ↗

19245.06d2Organizational.2-06.d 06.01 Compliance with Legal Requirements

ID: 19245.06d2Organizational.2-06.d Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Confirm quality and integrity of PII ↗	CMA_C1821 - Confirm quality and integrity of PII	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 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Evaluate and review PII holdings regularly ↗	CMA_C1832 - Evaluate and review PII holdings regularly	Manual, Disabled	1.1.0 ↗
Issue guidelines for ensuring data quality and integrity ↗	CMA_C1824 - Issue guidelines for ensuring data quality and integrity	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 ↗
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 ↗
Publish Computer Matching Agreements on public website ↗	CMA_C1829 - Publish Computer Matching Agreements on public website	Manual, Disabled	1.1.0 ↗

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](#).

MARS-E (US)

Article • 04/05/2023

MARS-E overview

In 2012, the [Centers for Medicare & Medicaid Services](#) (CMS) published the Minimum Acceptable Risk Standards for Exchanges (MARS-E) in accordance with CMS information security and privacy programs. The suite of documents, including guidance, requirements, and templates, was designed to address mandates of the Patient Protection and Affordable Care Act (ACA) and regulations of the Department of Health and Human Services (HHS) that apply to the ACA. The National Institute of Standards and Technology (NIST) [SP 800-53](#) *Security and Privacy Controls for Information Systems and Organizations* serves as the parent framework that establishes the security and compliance requirements for all systems, interfaces, and connections between ACA-mandated health exchanges and marketplaces.

Following the release of MARS-E, NIST released an update, SP 800-53 Rev. 4, to address growing challenges to online security, including application security; insider and advanced persistent threats; supply chain risks; and the trustworthiness, assurance, and resilience of systems of mobile and cloud computing. CMS then revised the MARS-E framework to align with the updated controls and parameters in NIST 800-53 Rev. 4, publishing MARS-E 2.0 in 2015. For more information, see [Minimum Acceptable Risk Standards](#).

The MARS-E 2.0 updates address the confidentiality, integrity, and availability of protected data in health exchanges, which includes personally identifiable information, protected health information, and federal tax information. The MARS-E 2.0 framework aims to secure this protected data and applies to all ACA administering entities, including exchanges or marketplaces, federal, state, state Medicaid, or Children's Health Insurance Program (CHIP) agencies, and their supporting contractors.

Azure and MARS-E

There's no formal authorization or certification process for MARS-E. However, the MARS-E framework is aligned with NIST SP 800-53 Rev. 4, which serves as the baseline control set for the US Federal Risk and Authorization Management Program (FedRAMP). Therefore, a FedRAMP assessment and authorization provides a strong foundation for evaluating MARS-E requirements mapped to NIST SP 800-53 controls.

- Microsoft maintains a [FedRAMP High authorization](#) for both Azure and Azure Government issued by the FedRAMP Joint Authorization Board (JAB). Although FedRAMP doesn't specifically focus on MARS-E, the MARS-E control requirements and objectives are very closely aligned with FedRAMP and serve to protect the confidentiality, integrity, and availability of data on Azure.
- An accredited third-party assessment organization (3PAO) has attested that both Azure and Azure Government meet the applicable requirements of MARS-E. The attestation was based on an analysis of the security controls defined in the MARS-E catalog to determine Azure and Azure Government compliance status based on existing assessments such as FedRAMP. The result of this analysis was that additional controls that are required as part of the MARS-E catalog were added to assessment scope to demonstrate compliance with the security controls defined in the MARS-E catalog.

Applicability

- Azure
- Azure Government

Attestation documents

For instructions on how to access attestation documents, see [Audit documentation](#). The following attestation letters are available from the Service Trust Portal (STP) [United States Government](#) section:

- Azure Commercial – Attestation of Compliance with MARS-E
- Azure Government – Attestation of Compliance with MARS-E

An accredited third-party assessment organization (3PAO) has attested that Azure (also known as Azure Commercial) and Azure Government comply with the security controls defined in the CMS MARS-E catalog.

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

Frequently asked questions

To whom does the standard apply?

MARS-E applies to all Affordable Care Act administering entities, including exchanges or marketplaces, federal, state, Medicaid, and CHIP agencies administering the Basic Health Program, as well as all their contractors and subcontractors.

How does Azure demonstrate adherence to this standard?

Using the formal FedRAMP assessment and authorization program, Microsoft is able to show how relevant controls in the underlying NIST SP 800-53 control baseline demonstrate Azure alignment with MARS-E security and privacy requirements. Starting with the FedRAMP control baseline, an accredited third-party assessment organization (3PAO) identified additional controls required for Azure and Government to demonstrate compliance with the security controls defined in the MARS-E catalog. After these additional controls were successfully tested, the 3PAO produced attestation letters to confirm that Azure and Azure Government meet the applicable MARS-E requirements.

How can I get the Azure MARS-E attestation documents?

For links to audit documentation, see [Attestation documents](#).

How can I use Microsoft's support for MARS-E in my own assessment?

You can review available Azure and Azure Government FedRAMP documentation for evidence of control effectiveness that Microsoft has implemented to maintain the security and privacy of the Azure platform. You may use the audited controls described in FedRAMP documentation as part of your own MARS-E compliance assessment. Microsoft doesn't inspect, approve, or monitor your applications deployed on Azure. You're wholly responsible for ensuring your own compliance with all applicable laws and regulations.

Resources

- [Azure compliance documentation](#)
- [Azure enables a world of compliance](#)
- [Microsoft 365 compliance offerings](#)
- [Compliance on the Microsoft Trust Center](#)
- [Centers for Medicare & Medicaid Services](#) (CMS)
- [CMS Minimum Acceptable Risk Standards](#)
- [Volume 2 MARS-E v2.0: Minimum Acceptable Risk Standards for Exchanges](#)
- [Volume 3 MARS-E v2.0: Catalog of Security and Privacy Controls](#)
- [FedRAMP documents and templates](#)
- [NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations](#)
- [Microsoft Cloud for healthcare compliance offerings](#)
- [Azure for healthcare](#)
- [Azure high-performance computing for health and life sciences](#)
- [Microsoft Cloud for healthcare](#)

Solutions for the government industry

Article • 11/15/2022

Microsoft Azure provides a mission-critical cloud platform, Azure Government, that delivers breakthrough innovation to US government customers and their partners. US federal, state, local, and tribal governments and their partners can have secure and dedicated access to this platform, with operations controlled by screened US citizens.

Using Azure Government, you can:

- test and deploy secure, highly-available, and performant mission-critical apps,
- create custom web experiences,
- gain insights from your data by using AI and analytics capabilities.

https://www.youtube-nocookie.com/embed/_WcyWeARD2Y

Azure Government offers a broad level of certifications to simplify critical government compliance requirements. To learn more about this government-focused cloud platform, visit [Azure Government](#).

Microsoft is committed to provide government agencies with innovative technology solutions across health and human services, critical infrastructure, public safety & justice, and tax, finance, and revenue. Learn more at [Cloud computing for government](#).

Architectures for government

The following articles provide detailed analysis of architectures developed and recommended for the government industry.

Architecture	Summary	Technology focus
Azure Automation in a hybrid environment	Extend automated management and configuration from Azure to on-premises and other cloud providers.	Hybrid/Multicloud
Azure Automation Update Management	Design a hybrid update management solution to manage updates on both Microsoft Azure and on-premises Windows and Linux computers.	Hybrid/Multicloud

Architecture	Summary	Technology focus
Computer forensics Chain of Custody in Azure	Ensure a valid Chain of Custody (CoC) in acquiring, storing, and accessing of digital evidence to support criminal investigations or civil proceedings.	Management/Governance
Hybrid Security Monitoring using Microsoft Defender for Cloud and Microsoft Sentinel	Monitor the security configuration and telemetry of on-premises and Azure operating system workloads.	Hybrid/Multicloud
Vision classifier model with Azure Custom Vision Cognitive Service	Combine AI and Internet of Things (IoT) by using Azure Custom Vision to classify images taken by a simulated drone.	AI/ML
Web app private connectivity to Azure SQL database	Set up private connectivity from an Azure Web App to Azure Platform-as-a-Service (PaaS) services.	Security
Azure Virtual Desktop for the enterprise	Use Azure Virtual Desktop to build virtualized desktop infrastructure (VDI) solutions at enterprise scale, covering 1,000 virtual desktops and above.	Hybrid/Multicloud

Solution ideas for government

The following article provides an idea that you can use as a starting point for your government solution.

- [DevSecOps in GitHub](#)

Compare Azure Government and global Azure

Article • 10/12/2023

Microsoft Azure Government uses same underlying technologies as global Azure, which includes the core components of [Infrastructure-as-a-Service \(IaaS\)](#), [Platform-as-a-Service \(PaaS\)](#), and [Software-as-a-Service \(SaaS\)](#). Both Azure and Azure Government have the same comprehensive security controls in place and the same Microsoft commitment on the safeguarding of customer data. Whereas both cloud environments are assessed and authorized at the FedRAMP High impact level, 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](#). These commitments may be of interest to customers using the cloud to store or process data subject to US export control regulations.

⚠ Note

These lists and tables do not include feature or bundle availability in the Azure Government Secret or Azure Government Top Secret clouds. For more information about specific availability for air-gapped clouds, please contact your account team.

Export control implications

You're responsible for designing and deploying your applications to meet [US export control requirements](#) such as the requirements prescribed in the EAR, ITAR, and DoE 10 CFR Part 810. In doing so, you shouldn't include sensitive or restricted information in Azure resource names, as explained in [Considerations for naming Azure resources](#).

Guidance for developers

Most of the currently available technical content assumes that applications are being developed on global Azure rather than on Azure Government. For this reason, it's important to be aware of two key differences in applications that you develop for hosting in Azure Government.

- Certain services and features that are in specific regions of global Azure might not be available in Azure Government.
- Feature configurations in Azure Government might differ from those in global Azure.

Therefore, it's important to review your sample code and configurations to ensure that you are building within the Azure Government cloud services environment.

For more information, see [Azure Government developer guide](#).

⚠ Note

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install the Azure Az PowerShell module](#).

You can use AzureCLI or PowerShell to obtain Azure Government endpoints for services you provisioned:

- Use **Azure CLI** to run the `az cloud show` command and provide `AzureUSGovernment` as the name of the target cloud environment. For example,

Azure CLI

```
az cloud show --name AzureUSGovernment
```

should get you different endpoints for Azure Government.

- Use a **PowerShell** cmdlet such as [Get-AzEnvironment](#) to get endpoints and metadata for an instance of Azure service. For example,

PowerShell

```
Get-AzEnvironment -Name AzureUSGovernment
```

should get you properties for Azure Government. This cmdlet gets environments from your subscription data file.

Table below lists API endpoints in Azure vs. Azure Government for accessing and managing some of the more common services. If you provisioned a service that isn't listed in the table below, see the Azure CLI and PowerShell examples above for suggestions on how to obtain the corresponding Azure Government endpoint.

[Expand table](#)

Service category	Service name	Azure Public	Azure Government	Notes
AI + machine learning	Azure Bot Service	botframework.com	botframework.azure.us	
	Azure AI Document Intelligence	cognitiveservices.azure.com	cognitiveservices.azure.us	
	Computer Vision	cognitiveservices.azure.com	cognitiveservices.azure.us	
	Custom Vision	cognitiveservices.azure.com	cognitiveservices.azure.us	Portal
	Content Moderator	cognitiveservices.azure.com	cognitiveservices.azure.us	
	Face API	cognitiveservices.azure.com	cognitiveservices.azure.us	
	Language Understanding	cognitiveservices.azure.com	cognitiveservices.azure.us	Portal Part of Azure AI Language
	Personalizer	cognitiveservices.azure.com	cognitiveservices.azure.us	
	QnA Maker	cognitiveservices.azure.com	cognitiveservices.azure.us	Part of Azure AI Language
	Speech service	See STT API docs	Speech Studio	
			See Speech service endpoints	
			Speech translation endpoints	
			Virginia:	
			https://usgovvirginia.s2s.speech.azure.us	

Service category	Service name	Azure Public	Azure Government	Notes
			Arizona: https://usgovarizona.s2s.speech.azure.us	
	Text Analytics	cognitiveservices.azure.com	cognitiveservices.azure.us	Part of Azure AI Language
	Translator	See Translator API docs	cognitiveservices.azure.us	
Analytics	Azure HDInsight	azurehdinsight.net	azurehdinsight.us	
	Event Hubs	servicebus.windows.net	servicebus.usgovcloudapi.net	
	Power BI	app.powerbi.com	app.powerbigov.us	Power BI US Gov
Compute	Batch	batch.azure.com	batch.usgovcloudapi.net	
	Cloud Services	cloudapp.net	usgovcloudapp.net	
Containers	Azure Service Fabric	cloudapp.azure.com	cloudapp.usgovcloudapi.net	
	Container Registry	azurecr.io	azurecr.us	
Databases	Azure Cache for Redis	redis.cache.windows.net	redis.cache.usgovcloudapi.net	See How to connect to other clouds
	Azure Cosmos DB	documents.azure.com	documents.azure.us	
	Azure Database for MariaDB	mariadb.database.azure.com	mariadb.database.usgovcloudapi.net	
	Azure Database for MySQL	mysql.database.azure.com	mysql.database.usgovcloudapi.net	
	Azure Database for PostgreSQL	postgres.database.azure.com	postgres.database.usgovcloudapi.net	
	Azure SQL Database	database.windows.net	database.usgovcloudapi.net	
Identity	Microsoft Entra ID	login.microsoftonline.com	login.microsoftonline.us	
		certauth.login.microsoftonline.com	certauth.login.microsoftonline.us	
		passwordreset.microsoftonline.com	passwordreset.microsoftonline.us	
Integration	Service Bus	servicebus.windows.net	servicebus.usgovcloudapi.net	
Internet of Things	Azure IoT Hub	azure-devices.net	azure-devices.us	
	Azure Maps	atlas.microsoft.com	atlas.azure.us	

Service category	Service name	Azure Public	Azure Government	Notes
	Notification Hubs	servicebus.windows.net	servicebus.usgovcloudapi.net	
Management and governance	Azure Automation	azure-automation.net	azure-automation.us	
	Azure Monitor	mms.microsoft.com	oms.microsoft.us	Log Analytics workspace portal
		ods.opinsights.azure.com	ods.opinsights.azure.us	Data collector API
		oms.opinsights.azure.com	oms.opinsights.azure.us	
		portal.loganalytics.io	portal.loganalytics.us	
		api.loganalytics.io	api.loganalytics.us	
		docs.loganalytics.io	docs.loganalytics.us	
		adx.monitor.azure.com	adx.monitor.azure.us	Data Explorer queries
Azure Resource Manager		management.azure.com	management.usgovcloudapi.net	
Cost Management		consumption.azure.com	consumption.azure.us	
Gallery URL		gallery.azure.com	gallery.azure.us	
Microsoft Azure portal		portal.azure.com	portal.azure.us	
Microsoft Intune		enterpriseregistration.windows.net	enterpriseregistration.microsoftonline.us	Enterprise registration
		manage.microsoft.com	manage.microsoft.us	Enterprise enrollment
Migration	Azure Site Recovery	hypervrecoverymanager.windowsazure.com	hypervrecoverymanager.windowsazure.us	Site Recovery service
		backup.windowsazure.com	backup.windowsazure.us	Protection service
		blob.core.windows.net	blob.core.usgovcloudapi.net	Storing VM snapshots
Networking	Traffic Manager	trafficmanager.net	usgovtrafficmanager.net	
Security	Key Vault	vault.azure.net	vault.usgovcloudapi.net	
Storage	Azure Backup	backup.windowsazure.com	backup.windowsazure.us	
	Blob	blob.core.windows.net	blob.core.usgovcloudapi.net	

Service category	Service name	Azure Public	Azure Government	Notes
Virtual desktop infrastructure	Queue	queue.core.windows.net	queue.core.usgovcloudapi.net	
	Table	table.core.windows.net	table.core.usgovcloudapi.net	
	File	file.core.windows.net	file.core.usgovcloudapi.net	
Azure Virtual Desktop	See AVD docs		See AVD docs	
Web	API Management	management.azure.com	management.usgovcloudapi.net	
	API Management Gateway	azure-api.net	azure-api.us	
	API Management management	management.azure-api.net	management.azure-api.us	
	API Management Portal	portal.azure-api.net	portal.azure-api.us	
Cloud services	App Configuration	azconfig.io	azconfig.azure.us	
	App Service	azurewebsites.net	azurewebsites.us	
	Azure AI Search	search.windows.net	search.windows.us	
	Azure Functions	azurewebsites.net	azurewebsites.us	

Service availability

Microsoft's goal for Azure Government is to match service availability in Azure. For service availability in Azure Government, see [Products available by region](#). Services available in Azure Government are listed by category and whether they're Generally Available or available through Preview. If a service is available in Azure Government, that fact isn't reiterated in the rest of this article. Instead, you're encouraged to review [Products available by region](#) for the latest, up-to-date information on service availability.

In general, service availability in Azure Government implies that all corresponding service features are available to you. Variations to this approach and other applicable limitations are tracked and explained in this article based on the main service categories outlined in the [online directory of Azure services](#). Other considerations for service deployment and usage in Azure Government are also provided.

AI + machine learning

This section outlines variations and considerations when using **Azure Bot Service**, **Azure Machine Learning**, and **Cognitive Services** in the Azure Government environment. For service availability, see [Products available by region](#).

Azure Bot Service

The following Azure Bot Service **features aren't currently available** in Azure Government:

- Bot Framework Composer integration
- Channels (due to availability of dependent services)
 - Direct Line Speech Channel
 - Telephony Channel (Preview)
 - Microsoft Search Channel (Preview)
 - Kik Channel (deprecated)

For information on how to deploy Bot Framework and Azure Bot Service bots to Azure Government, see [Configure Bot Framework bots for US Government customers](#).

Azure Machine Learning

For feature variations and limitations, see [Azure Machine Learning feature availability across cloud regions](#).

Azure AI services: Content Moderator

The following Content Moderator **features aren't currently available** in Azure Government:

- Review UI and Review APIs.

Azure AI Language Understanding (LUIS)

The following Language Understanding **features aren't currently available** in Azure Government:

- Speech Requests
- Prebuilt Domains

Azure AI Language Understanding (LUIS) is part of [Azure AI Language](#).

Azure AI Speech

For feature variations and limitations, including API endpoints, see [Speech service in sovereign clouds](#).

Azure AI services: Translator

For feature variations and limitations, including API endpoints, see [Translator in sovereign clouds](#).

Analytics

This section outlines variations and considerations when using Analytics services in the Azure Government environment. For service availability, see [Products available by region](#).

Azure HDInsight

For secured virtual networks, you'll want to allow network security groups (NSGs) access to certain IP addresses and ports. For Azure Government, you should allow the following IP addresses (all with an Allowed port of 443):

 [Expand table](#)

Region	Allowed IP addresses	Allowed port
US DoD Central	52.180.249.174 52.180.250.239	443

Region	Allowed IP addresses	Allowed port
US DoD East	52.181.164.168 52.181.164.151	443
US Gov Texas	52.238.116.212 52.238.112.86	443
US Gov Virginia	13.72.49.126 13.72.55.55 13.72.184.124 13.72.190.110	443
US Gov Arizona	52.127.3.176 52.127.3.178	443

For a demo on how to build data-centric solutions on Azure Government using HDInsight, see Azure AI services, HDInsight, and Power BI on Azure Government.

Power BI

For usage guidance, feature variations, and limitations, see [Power BI for US government customers](#). For a demo on how to build data-centric solutions on Azure Government using Power BI, see Azure AI services, HDInsight, and Power BI on Azure Government.

Power BI Embedded

To learn how to embed analytical content within your business process application, see [Tutorial: Embed a Power BI content into your application for national clouds](#).

Databases

This section outlines variations and considerations when using Databases services in the Azure Government environment. For service availability, see [Products available by region](#).

Azure Database for MySQL

The following Azure Database for MySQL **features aren't currently available** in Azure Government:

- Advanced Threat Protection

Azure Database for PostgreSQL

For Flexible Server availability in Azure Government regions, see [Azure Database for PostgreSQL – Flexible Server](#).

The following Azure Database for PostgreSQL **features aren't currently available** in Azure Government:

- Azure Cosmos DB for PostgreSQL, formerly Azure Database for PostgreSQL – Hyperscale (Citus). For more information about supported regions, see [Regional availability for Azure Cosmos DB for PostgreSQL](#).
- The following features of the Single Server deployment option
 - Advanced Threat Protection
 - Backup with long-term retention

Developer tools

This section outlines variations and considerations when using Developer tools in the Azure Government environment. For service availability, see [Products available by region](#).

Enterprise Dev/Test subscription offer

- Enterprise Dev/Test subscription offer in existing or separate tenant is currently available only in Azure public as documented in [Azure EA portal administration](#).

Identity

This section outlines variations and considerations when using Identity services in the Azure Government environment. For service availability, see [Products available by region](#).

Microsoft Entra ID P1 and P2

For feature variations and limitations, see [Cloud feature availability](#).

For information on how to use Power BI capabilities for collaboration between Azure and Azure Government, see [Cross-cloud B2B](#).

The following features have known limitations in Azure Government:

- Limitations with B2B Collaboration in supported Azure US Government tenants:
 - For more information about B2B collaboration limitations in Azure Government and to find out if B2B collaboration is available in your Azure Government tenant, see [Microsoft Entra B2B in government and national clouds](#).
- Limitations with multi-factor authentication:
 - Trusted IPs isn't supported in Azure Government. Instead, use Conditional Access policies with named locations to establish when multi-factor authentication should and shouldn't be required based off the user's current IP address.

Azure Active Directory B2C

Azure Active Directory B2C is **not available** in Azure Government.

Microsoft Authentication Library (MSAL)

The Microsoft Authentication Library (MSAL) enables developers to acquire security tokens from the Microsoft identity platform to authenticate users and access secured web APIs. For feature variations and limitations, see [National clouds and MSAL](#).

Management and governance

This section outlines variations and considerations when using Management and Governance services in the Azure Government environment. For service availability, see [Products available by region](#).

Automation

The following Automation features aren't currently available in Azure Government:

- Automation analytics solution

Azure Advisor

For feature variations and limitations, see [Azure Advisor in sovereign clouds](#).

Azure Lighthouse

The following Azure Lighthouse **features aren't currently available** in Azure Government:

- Managed Service offers published to Azure Marketplace
- Delegation of subscriptions across a national cloud and the Azure public cloud, or across two separate national clouds, isn't supported
- Privileged Identity Management (PIM) feature isn't enabled, for example, just-in-time (JIT) / eligible authorization capability

Azure Monitor

Azure Monitor enables the same features in both Azure and Azure Government.

- System Center Operations Manager 2019 is supported equally well in both Azure and Azure Government.

The following options are available for previous versions of System Center Operations Manager:

- Integrating System Center Operations Manager 2016 with Azure Government requires an updated Advisor management pack that is included with Update Rollup 2 or later.
- System Center Operations Manager 2012 R2 requires an updated Advisor management pack included with Update Rollup 3 or later.

For more information, see [Connect Operations Manager to Azure Monitor](#).

Frequently asked questions

- Can I migrate data from Azure Monitor logs in Azure to Azure Government?
 - No. It isn't possible to move data or your workspace from Azure to Azure Government.
- Can I switch between Azure and Azure Government workspaces from the Operations Management Suite portal?
 - No. The portals for Azure and Azure Government are separate and don't share information.

Application Insights

Application Insights (part of Azure Monitor) enables the same features in both Azure and Azure Government. This section describes the supplemental configuration that is required to use Application Insights in Azure Government.

Visual Studio – In Azure Government, you can enable monitoring on your ASP.NET, ASP.NET Core, Java, and Node.js based applications running on Azure App Service. For more information, see [Application monitoring for Azure App Service overview](#). In Visual Studio, go to Tools|Options|Accounts|Registered Azure Clouds|Add New Azure Cloud and select Azure US Government as the Discovery endpoint. After that, adding an account in File|Account Settings will prompt you for which cloud you want to add from.

SDK endpoint modifications – In order to send data from Application Insights to an Azure Government region, you'll need to modify the default endpoint addresses that are used by the Application Insights SDKs. Each SDK requires slightly different modifications, as described in [Application Insights overriding default endpoints](#).

Firewall exceptions – Application Insights uses several IP addresses. You might need to know these addresses if the app that you're monitoring is hosted behind a firewall. For more information, see [IP addresses used by Azure Monitor](#) from where you can download Azure Government IP addresses.

⚠ Note

Although these addresses are static, it's possible that we'll need to change them from time to time. All Application Insights traffic represents outbound traffic except for availability monitoring and webhooks, which require inbound firewall rules.

You need to open some **outgoing ports** in your server's firewall to allow the Application Insights SDK and/or Status Monitor to send data to the portal:

 [Expand table](#)

Purpose	URL	IP address	Ports
Telemetry	dc.applicationinsights.us	23.97.4.113	443

Cost Management and Billing

The following Azure Cost Management + Billing **features aren't currently available** in Azure Government:

- Cost Management + Billing for cloud solution providers (CSPs)

Media

This section outlines variations and considerations when using Media services in the Azure Government environment. For service availability, see [Products available by region](#).

Media Services

For Azure Media Services v3 feature variations in Azure Government, see [Azure Media Services v3 clouds and regions availability](#).

Migration

This section outlines variations and considerations when using Migration services in the Azure Government environment. For service availability, see [Products available by region](#).

Azure Migrate

The following Azure Migrate **features aren't currently available** in Azure Government:

- Containerizing Java Web Apps on Apache Tomcat (on Linux servers) and deploying them on Linux containers on App Service.
- Containerizing Java Web Apps on Apache Tomcat (on Linux servers) and deploying them on Linux containers on Azure Kubernetes Service (AKS).
- Containerizing ASP.NET apps and deploying them on Windows containers on AKS.
- Containerizing ASP.NET apps and deploying them on Windows containers on App Service.
- You can only create assessments for Azure Government as target regions and using Azure Government offers.

For more information, see [Azure Migrate support matrix](#). For a list of Azure Government URLs needed by the Azure Migrate appliance when connecting to the internet, see [Azure Migrate appliance URL access](#).

Networking

This section outlines variations and considerations when using Networking services in the Azure Government environment. For service availability, see [Products available by region](#).

Azure ExpressRoute

For an overview of ExpressRoute, see [What is Azure ExpressRoute?](#). For an overview of how **BGP communities** are used with ExpressRoute in Azure Government, see [BGP community support in National Clouds](#).

Azure Front Door

Azure Front Door (AFD) Standard and Premium tiers are available in general availability in Azure Government regions US Gov Arizona and US Gov Texas. The following Azure Front Door feature **isn't supported** in Azure Government:

- Managed certificate for enabling HTTPS; instead use your own certificate.

Private Link

- For Private Link services availability, see [Azure Private Link availability](#).
- For Private DNS zone names, see [Azure Private Endpoint DNS configuration](#).

Traffic Manager

Traffic Manager health checks can originate from certain IP addresses for Azure Government. Review the [IP addresses in the JSON file](#) to ensure that incoming connections from these IP addresses are allowed at the endpoints to check its health status.

Security

This section outlines variations and considerations when using Security services in the Azure Government environment. For service availability, see [Products available by region](#).

Microsoft Defender for Endpoint

For feature variations and limitations, see [Microsoft Defender for Endpoint for US Government customers](#).

Microsoft Defender for IoT

For feature variations and limitations, see [Cloud feature availability for US Government customers](#).

Azure Information Protection

Azure Information Protection Premium is part of the [Enterprise Mobility + Security](#) suite. For details on this service and how to use it, see [Azure Information Protection Premium Government Service Description](#).

Microsoft Defender for Cloud

For feature variations and limitations, see [Cloud feature availability for US Government customers](#).

Microsoft Sentinel

For feature variations and limitations, see [Cloud feature availability for US Government customers](#).

Storage

This section outlines variations and considerations when using Storage services in the Azure Government environment. For service availability, see [Products available by region](#).

Azure NetApp Files

For Azure NetApp Files feature availability in Azure Government and how to access the Azure NetApp Files service within Azure Government, see [Azure NetApp Files for Azure Government](#).

Azure Import/Export

With Import/Export jobs for US Gov Arizona or US Gov Texas, the mailing address is for US Gov Virginia. The data is loaded into selected storage accounts from the US Gov Virginia region. For all jobs, we recommend that you rotate your storage account keys after the job is complete to remove any access granted during the process. For more information, see [Manage storage account access keys](#).

Web

This section outlines variations and considerations when using Web services in the Azure Government environment. For service availability, see [Products available by region](#).

API Management

The following API Management **features aren't currently available** in Azure Government:

- Azure AD B2C integration

App Service

The following App Service **resources aren't currently available** in Azure Government:

- App Service Certificate
- App Service Managed Certificate
- App Service Domain

The following App Service **features aren't currently available** in Azure Government:

- Deployment
 - Deployment options: only Local Git Repository and External Repository are available

Azure Functions

When connecting your Functions app to Application Insights in Azure Government, make sure you use `APPLICATIONINSIGHTS_CONNECTION_STRING`, which lets you customize the Application Insights endpoint.

Next steps

Learn more about Azure Government:

- [Acquiring and accessing Azure Government ↗](#)
- [Azure Government overview](#)
- [Azure support for export controls](#)
- [Azure Government compliance](#)
- [Azure Government security](#)
- [Azure guidance for secure isolation](#)

Start using Azure Government:

- [Guidance for developers](#)
- [Connect with the Azure Government portal](#)

Dynamics 365 government accelerator

Article • 12/15/2023

ISVs, partners, and developers can use the Dynamics 365 government accelerator to build solutions for government organizations to advance their missions in the following areas:

- Public finance
- Public health and social services
- Public safety and justice
- Critical infrastructure

The accelerator acts as an information blueprint. It includes an industry-specific data model and building blocks for use in government business processes and applications.

The accelerator expands the Common Data Model to include a government data model with a standardized data schema. The schema includes tables, columns, metadata, and relationships to support government use cases, including programs, services, and benefits. This standardized data blueprint improves interoperability by unifying and shaping the data in a consistent form to use across applications, processes, and workflows in Microsoft Power Platform and Microsoft Dynamics 365. With a shared understanding of the data, partners and developers accelerate their time to value to deliver mission-focused solutions for government agencies.

The government accelerator provides the following features to use for government organizations and agencies:

- Government-specific extensions to [Common Data Model \(CDM\)](#), including a data model to support government segments.
- A sample customizable app for government services, programs, and benefits. The app shows how Microsoft Power Platform and Dynamics 365 can use the data model to manage applications and approvals, and to transform government programs and services.
- A sample customizable Power Apps portal for residents and businesses to apply for government services, programs, and benefits.
- Front-office to back-office program and fund management that includes the following processes:
 - Applicants find out about a government program
 - Applicants apply for a benefit
 - Approvals

- Tracking against the associated fund and budget in [Dynamics 365 Finance for public sector](#)
- Partner and developer documentation on [GitHub](#). The documentation includes reference guides, entity relationship diagrams (ERDs), and metadata documentation on the data model.

Industry data model for government

The government accelerator comes with an industry data model that you can use in Power Platform and Dynamics 365 and across the Microsoft technology stack. The data model is a combination of relationships to native tables and government-specific tables, including:

- Government programs
- Services
- Benefits
- Eligibility
- Licenses
- Permits
- Grants

You can extend these data elements to build industry-leading, low-code or no-code applications on Power Platform. We built the government data model in collaboration with our partner and developer community. It's available as a standalone data model that ISVs and partners can use and build upon.

Tables and workflows

The government accelerator provides a data model to support the needs of government organizations in the areas of public finance, public health and social services, public safety and justice, and critical infrastructure.

- Application
- Application Process
- Application Type
- Building Permit Application
- Business Grant Application
- Business License Application
- Government Organization
- Grant

- Housing Benefit Application
- License
- Permit
- Program
- Program Benefit
- Program Eligibility Requirement
- Program Participant
- Program Type
- Public Policy
- Service
- Service Recipient
- Service Type
- Recipient

Government connections

The government accelerator provides a better view of the different personas in a government organization who are involved in government programs and services. It includes a set of connections that provide a flexible way to connect and describe the relationships used in a government process or workflow. The following example connections are included in the government accelerator.

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

Connection roles from contact to service	Connection roles from contact to program
Service Agent	Program Coordinator
Service Deputy	Program Manager
Service Manager	Program Director

Government services app

The accelerator includes a customizable sample app, workflows, and dashboards that showcase canonical programs of government agencies, including grant management, housing assistance, building permits, and business licenses. The app shows how government agencies can manage applications, eligibility, and approvals of government programs, services, and benefits.

The screenshot shows a Microsoft Power Apps interface for 'Government Services'. The main content area displays a detailed view of an application for 'Music hall impacted by COVID-19'. The application status is 'Approved'. The timeline on the right shows the following stages: 'Submitted', 'In Progress', 'In Review', 'Reviewed', and 'Complete'. The 'In Progress' stage is currently active. The 'Timeline' section allows users to add notes. A 'Get started' section encourages users to capture and manage all records in their timeline.

The screenshot shows a Microsoft Power Apps interface for 'Government Services' with a dashboard view. The dashboard includes several data visualizations: a pie chart for 'Active Applications' by type, a pie chart for 'Active Applications' by status, a pie chart for 'All Application Process' by stage, a bar chart for 'Active Applications' by program, a bar chart for 'Active Applications' by service, and a bar chart for 'Application Over Time By Month'.

Government portal

The government portal provides a customizable sample portal for a fictitious Contoso County. The portal allows residents and businesses to apply for government services, programs, and benefits.



Business



Licenses & Permits



Housing



Safety & Justice



Environmental



Jobs & Training



Coming soon



Coming soon



Coming soon

Additional resources

- The government accelerator is provided as part of the open-source creative license, available on [GitHub](#) ↗.
- This [Dynamics 365 blog post](#) ↗ includes more info and partners working with us on the Common Data Model for Government.

Configure Dynamics 365 government accelerator portal

Article • 12/15/2023

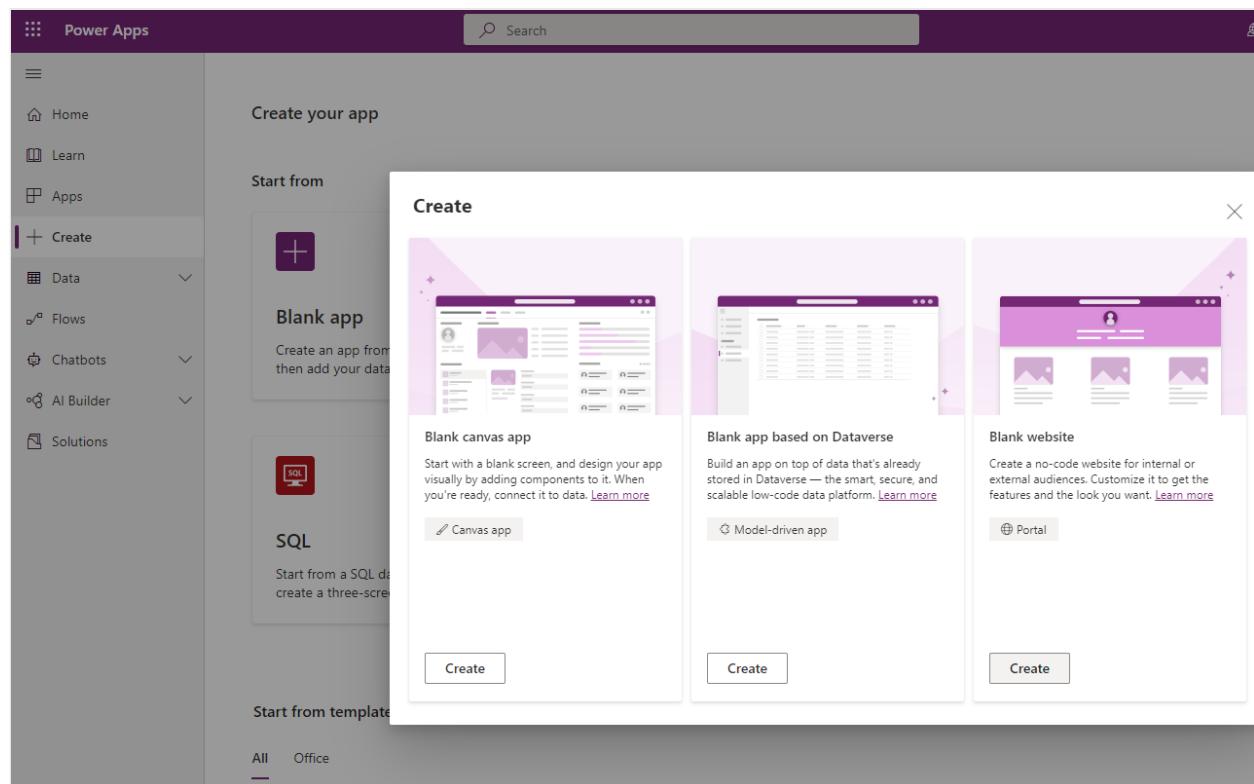
After you've installed the Microsoft Dynamics 365 government accelerator from Microsoft AppSource, follow these steps to enable and activate the government portal.

The government portal customizes Microsoft Power Apps portals to provide a customizable sample portal for a fictitious Contoso County. The portal allows residents and businesses to apply for government services, programs, and benefits. Applicants can log into the portal and see the status of their applications. They can also see any government programs and services they've received, including business licenses, permits, benefits, and grants.

Pre-deployment: Set up a new blank portal

Before you can deploy the portal, you need to set up a new website from blank:

1. Sign in to [Microsoft Power Apps](#).
2. Select **Create** in the left pane, select **Blank app**, and then select **Blank website**.



1. In the **Portal from blank** window, enter a **Name** for the portal and an **Address** for the website, and then select a **Language** from the dropdown list. When you're

done, select **Create**.

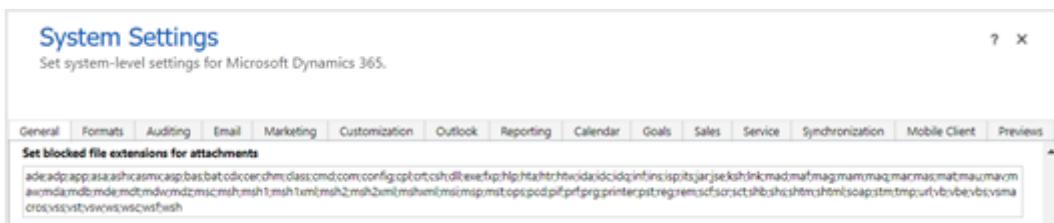
2. Update the system settings to allow JavaScript (.js) and cascading style sheet (.css) files:

- a. Select **Settings** (sprocket icon) in the upper-right corner, and then select **Advanced Settings**.

b. Select **Administration** in the System area group.

c. Select System Settings.

d. On the **General** tab, in the **Set blocked file extension for attachments** section, remove the .js and .css file extensions.



Post-deployment: Configure your portal

After you've installed the government solution, configure the portal.

Follow these steps to update the portal binding:

1. Select **Apps** in the left pane, locate the newly created portal, and then select the ellipses (...) to select **Settings**.

2. Within **Portal Settings**, under **Advanced Settings**, select the **Administration** link, which opens in a new window or tab.

3. Within Portal Details, find Update Portal Binding.

4. Change Select Website Record to Government Services.

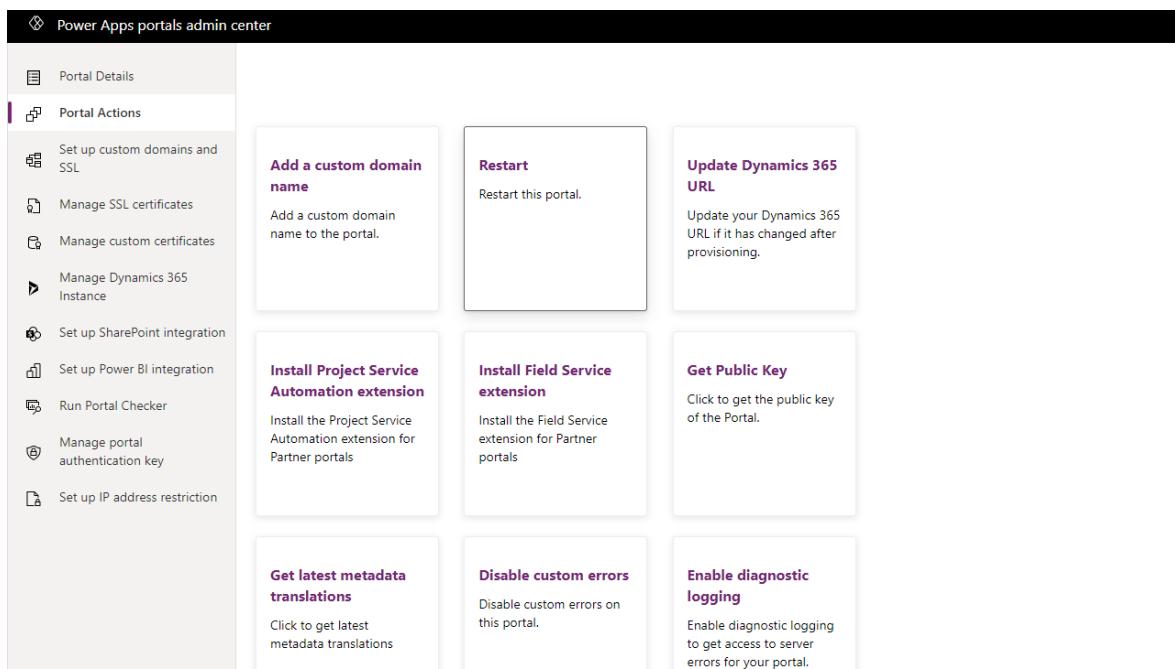
5. Select **Update**.

After this change, it might take up to five minutes for the website binding data to sync. Wait a few minutes before attempting to open the portal URL.

Remember to restart your portal for your customizations to take effect immediately. To restart a portal:

1. Open Power Apps portals admin center.

2. Select Portal Actions > Restart.



The screenshot shows the 'Power Apps Portals admin center' interface. On the left, a sidebar lists various portal management tasks. The 'Portal Actions' section is expanded, showing options like 'Set up custom domains and SSL', 'Manage SSL certificates', and 'Restart'. The 'Restart' option is highlighted with a purple border. Other visible options include 'Update Dynamics 365 URL', 'Install Project Service Automation extension', 'Install Field Service extension', 'Get Public Key', 'Get latest metadata translations', 'Disable custom errors', and 'Enable diagnostic logging'.

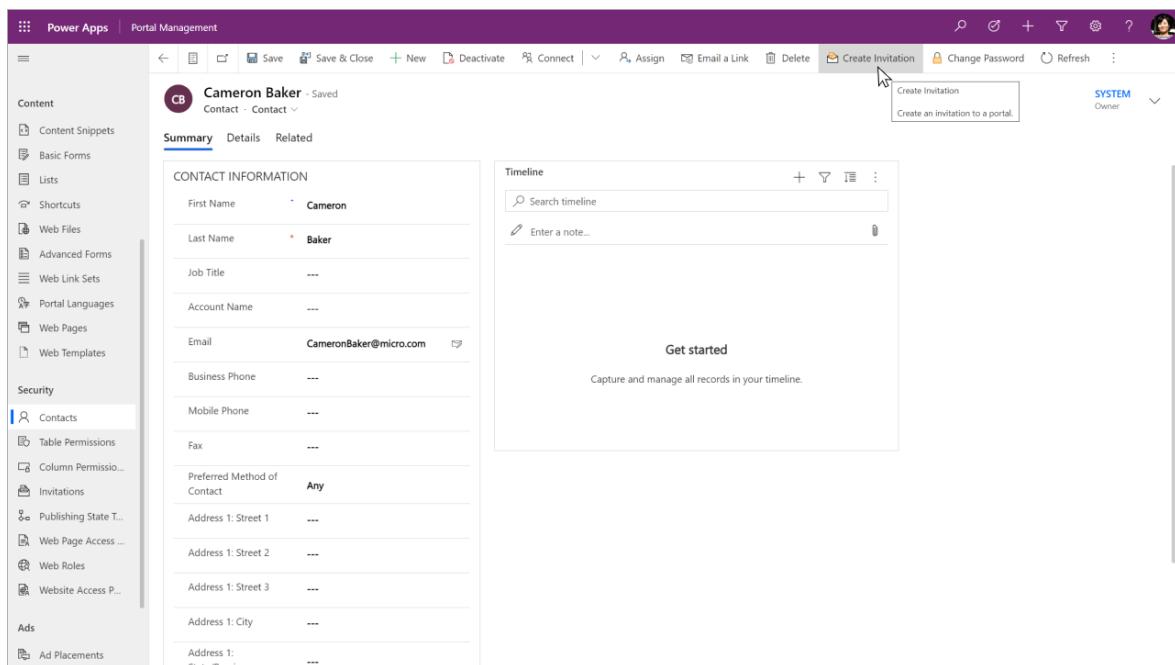
You can test out your portal in test and demo environments by including sample data while installing the portal solution. Set up a sign-in in the test portal for Cameron Baker, a fictitious resident of Contoso County.

1. Navigate to the **Portal Management** model-driven app.

2. Select **Contacts** in the sitemap.

3. Navigate to Cameron Baker's contact form.

4. On the command menu, select **Create Invitation**.



The screenshot shows the 'Power Apps | Portal Management' contact form for 'Cameron Baker'. The left sidebar shows the 'Content' section with various sub-options like 'Basic Forms', 'Lists', and 'Table Permissions'. The main area displays 'CONTACT INFORMATION' with fields for First Name (Cameron), Last Name (Baker), and Email (CameronBaker@micro.com). To the right is a 'Timeline' section with a search bar and a note input field. At the top right, there is a command menu with a 'Create Invitation' button, which is highlighted with a purple border. The status bar at the bottom right shows the user is a 'SYSTEM Owner'.

5. On the **Invitation** form, select **Save**.

6. Navigate to the **Advanced** tab on the **Invitation** form.
7. Copy the invitation code to your clipboard.
8. Navigate to **Government Portal**.
9. Select **Sign In**.
10. Select **Redeem Invitation**.
11. Paste in the invitation code and select **Register**.
12. Complete registration by entering a username and a password, and then select **Save**.
13. Confirm the user details in the portal.
14. Navigate to the **My Activity** section of the portal to view Cameron Baker's applications, previous service requests, benefits, and more.

You can use Power Apps portals Studio to create and customize your website. For more information, go to [Power Apps portals Studio anatomy](#).

To learn more about how to align your portal more to your organization, go to [Overview of themes in Power Apps portals](#).

Considerations for naming Azure resources

Article • 01/31/2022

You shouldn't include sensitive or restricted information in Azure resource names because it may be stored or accessed outside the compliance boundary to facilitate support and troubleshooting. Examples of sensitive information include data subject to:

- [Export control laws](#)
- [DoD Impact Level 5 isolation requirements](#)
- [Controlled Unclassified Information \(CUI\)](#) that warrants extra protection or is subject to NOFORN marking
- And others

Data stored or processed in customer VMs, storage accounts, databases, Azure Import/Export, Azure Cache for Redis, ExpressRoute, Azure AI Search, App Service, API Management, and other Azure services suitable for holding, processing, or transmitting customer data can contain sensitive data. However, metadata for these Azure services isn't permitted to contain sensitive or restricted data. This metadata includes all configuration data entered when creating and maintaining an Azure service, including:

- Subscription names, service names, server names, database names, tenant role names, resource groups, deployment names, resource names, resource tags, circuit name, and so on.
- All shipping information that is used to transport media for Azure Import/Export, such as carrier name, tracking number, description, return information, drive list, package list, storage account name, container name, and so on.
- Data in HTTP headers sent to the REST API in search/query strings as part of the API.
- Device/policy/application and [other metadata](#) sent to Intune.

Azure resource names include information provided by you, or on your behalf, that is used to identify or configure cloud service resources, such as software, systems, or containers. However, it does **not** include customer-created content or metadata inside the resource (for example, database column/table names). Azure resource names include the names you assign to Azure Resource Manager level objects and resources deployed in Azure. Examples include the names of resources such as virtual networks, virtual hard disks, database servers and databases, virtual network interface, network security groups, key vaults, and others.

ⓘ Note

The above examples are but a subset of the types of resources you can name. This list is not meant to be fully exhaustive and the types of resources could change in the future as new cloud services are added.

Naming convention

The names of Azure resources are part of a larger resource ID as follows:

```
/subscriptions/<subscriptionID>/resourceGroups/<ResourceGroupName>/providers/<ResourceProvider>/<ResourceType>/<ResourceName>
```

An example of a virtual machine resource ID is:

```
/subscriptions/<subscriptionID>/resourceGroups/<ResourceGroupName>/providers/Microsoft.Compute/virtualMachines/<virtualMachineName>
```

Naming considerations

You should avoid names that are sensitive to business or mission functions. This guidance applies to all names that meet the criteria mentioned previously, from the name of the larger resource group to the name of the end resources within it. You should also avoid names that indicate your regulatory requirements, for example:

- [Criminal Justice Information Services \(CJIS\)](#)
- [Committee on National Security Systems Instruction No. 1253 \(CNSSI 1253\)](#)
- [Internal Revenue Service \(IRS\) Publication 1075](#)
- [Export Administration Regulations \(EAR\)](#)
- [International Traffic in Arms Regulations \(ITAR\)](#)
- And others as applicable

ⓘ Note

Also consider naming of resource tags when reviewing the [Resource naming and tagging decision guide](#).

You should understand and take into account the resource naming convention to help ensure operational security, as Microsoft personnel could use the full resource ID in the following example scenarios:

- Microsoft support personnel may use the full resource ID of resources during support events to ensure we're identifying the right resource within a customer's subscription.
- Microsoft product engineering personnel could use full resource IDs during routine monitoring of telemetry data to identify deviations from baseline or average system performance.
- Proactive communication to customers about impacted resources during internally discovered incidents.

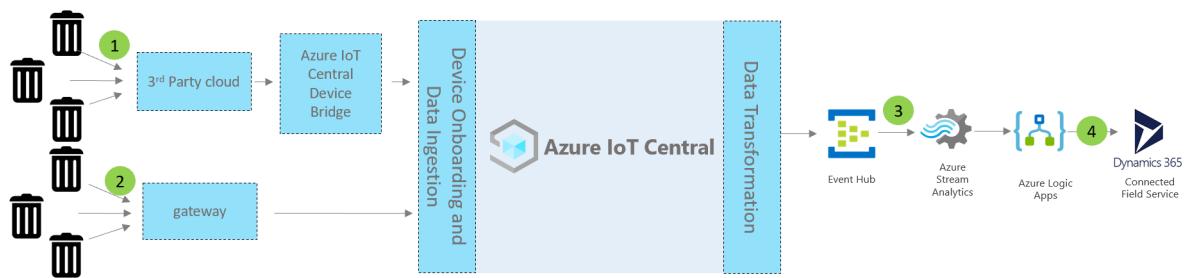
Next steps

- [Develop your naming and tagging strategy for Azure resources](#)
- [Resource naming and tagging decision guide](#)
- [Azure Government compliance](#)
- [Azure Government security](#)
- [Azure compliance](#)
- [Azure and other Microsoft services compliance offerings](#)

Tutorial: Deploy and walk through the connected waste management application template

Article • 07/17/2023

The *connected waste management* application template helps you kickstart your IoT solution development to remotely monitor to maximize efficient waste collection as part of a smart city.



Devices and connectivity (1,2)

Devices such as waste bins that are used in open environments may connect through low-power wide area networks or through a third-party network operator. For these types of devices, use the [Azure IoT Central Device Bridge](#) to send your device data to your IoT Central application. You can also use an IP capable device gateway that connects directly to your IoT Central application.

IoT Central

Azure IoT Central is an IoT App platform that helps you quickly build and deploy an IoT solution. You can brand, customize, and integrate your solution with third-party services.

When you connect your smart waste devices to IoT Central, the application provides:

- Device command and control.
- Monitoring and alerting.

- A user interface with built-in role-based access controls.
- Configurable dashboards.
- Extensibility options.

Extensibility and integrations (3)

You can extend your IoT application in IoT Central and optionally:

- Transform and integrate your IoT data for advanced analytics through data export from your IoT Central application.
- Automate workflows in other systems by triggering actions using Power Automate or webhooks from IoT Central application.
- Programmatically access your IoT Central application by using the IoT Central REST APIs.

Business applications (4)

You can use IoT data to power various business applications within a waste utility. For example, in a connected waste management solution you can optimize the dispatch of trash collections trucks. The optimization can be done based on IoT sensors data from connected waste bins. In your IoT Central connected waste management application, you can configure rules and actions and set them to create alerts in [Connected Field Service](#). Configure Power Automate in IoT Central rules to automate workflows across applications and services. Additionally, based on service activities in Connected Field Service, information can be sent back to Azure IoT Central.

You can easily configure the following integration processes with IoT Central and Connected Field Service:

- Azure IoT Central can send information about device anomalies to Connected Field Service for diagnosis.
- Connected Field Service can create cases or work orders triggered from device anomalies.
- Connected Field Service can schedule technicians for inspection to prevent the downtime incidents.
- Azure IoT Central device dashboard can be updated with relevant service and scheduling information.

In this tutorial, you learn how to:

- ✓ Use the Azure IoT Central *connected waste management* application template to create your app.

- ✓ Explore and customize the dashboard.
- ✓ Explore the connected waste bin device template.
- ✓ Explore simulated devices.
- ✓ Explore and configure rules.
- ✓ Configure jobs.
- ✓ Customize your application branding.

Prerequisites

An active Azure subscription. If you don't have an Azure subscription, create a [free account](#) before you begin.

Create connected waste management application

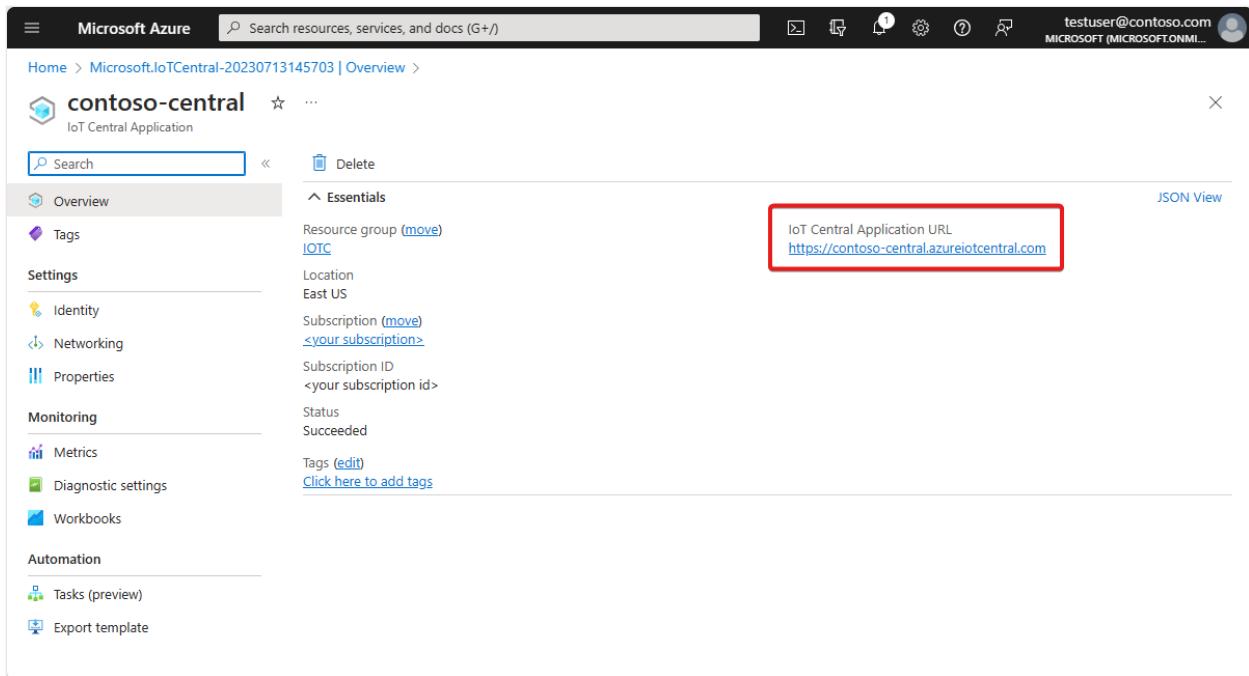
To create your IoT Central application:

1. Navigate to the [Create IoT Central Application](#) page in the Azure portal. If prompted, sign in with your Azure account.
2. Enter the following information:

Field	Description
Subscription	The Azure subscription you want to use.
Resource group	The resource group you want to use. You can create a new resource group or use an existing one.
Resource name	A valid Azure resource name.
Application URL	The URL subdomain for your application. The URL for an IoT Central application looks like <code>https://yoursubdomain.azureiotcentral.com</code> .
Template	Connected Waste Management
Region	The Azure region you want to use.
Pricing plan	The pricing plan you want to use.

3. Select **Review + create**. Then select **Create**.

When the app is ready, you can navigate to it from the Azure portal:



contoso-central

IoT Central Application

Search

Delete

Overview

Tags

Settings

- Identity
- Networking
- Properties

Monitoring

- Metrics
- Diagnostic settings
- Workbooks

Automation

- Tasks (preview)
- Export template

Resource group (move)
IOTC

Location
East US

Subscription (move)
<your subscription>

Subscription ID
<your subscription id>

Status
Succeeded

Tags (edit)
[Click here to add tags](#)

IoT Central Application URL
<https://contoso-central.azureiotcentral.com>

JSON View

💡 Tip

To list all the IoT Central applications you have access to, navigate to [IoT Central Applications](#).

To learn more, see [Create an Azure IoT Central application](#).

Walk through the application

The following sections walk you through the key features of the application:

Dashboard

After you deploy the application template, your default dashboard is **Wide World waste management dashboard**.

The screenshot shows the Azure IoT Central interface for a waste management application. The left sidebar has sections for Connect, Analyze, and Manage, with 'Dashboards' currently selected. The main area displays a dashboard titled 'Wide World waste management dashboard'. It includes a large image tile for 'WIDE WORLD WASTE UTILITY', a waste bin image tile labeled 'Waste bin 1 Connected waste bin.', and four KPI tiles for 'Bin 1'. The KPI tiles show 'Bin 1 info' (Last collect...No Value), 'Bin 1 fill level' (89%, 1 minute ago), 'Bin 1 tilt sensor' (320.10, 1 minute ago), and 'Bin 1 weight' (62.76, 1 minute ago). A fourth KPI tile shows 'Bin 1 fill, odor, weight levels' with a bar chart for Fill level (~50), Odor level (~40), and Weight (~60). A 'Waste monitoring area map' tile shows the world map with oceans labeled: Ocean, Atlantic Ocean, and Indian Ocean. A 'Field Service' card is also visible on the right.

As a builder, you can create and customize views on the dashboard for operators.

ⓘ Note

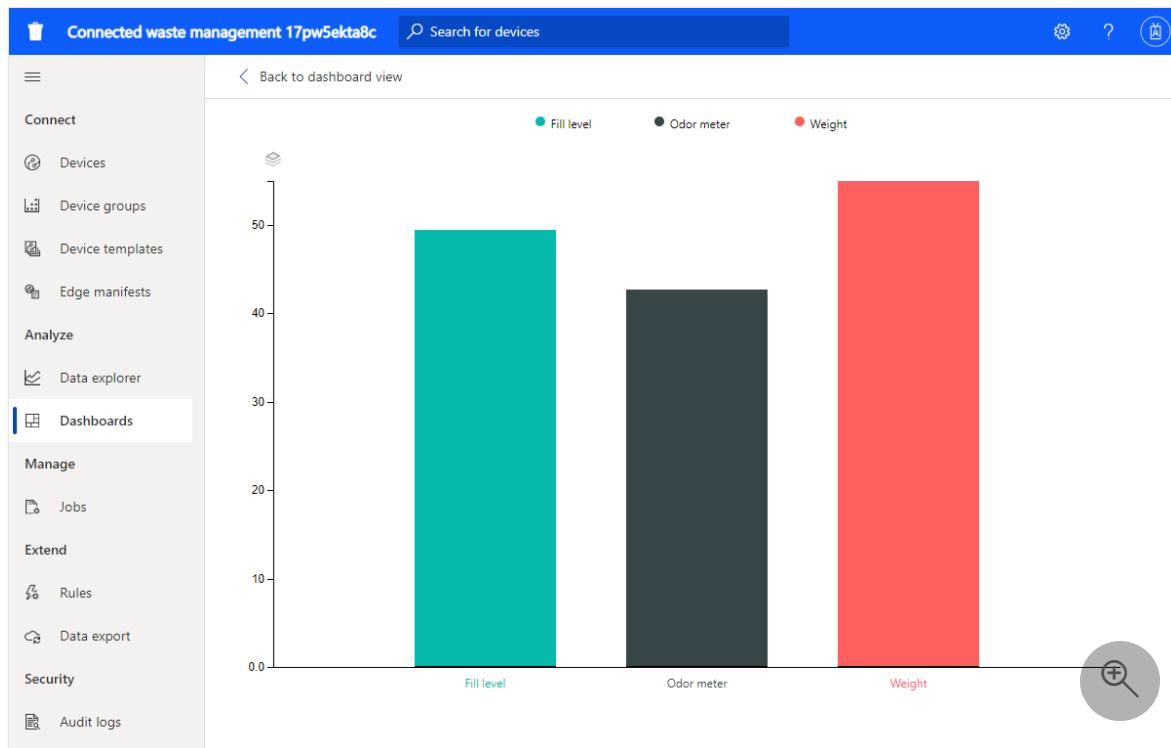
All data shown in the dashboard is based on simulated device data, which you see more of in the next section.

The dashboard consists of different tiles:

- **Wide World Waste utility image tile:** The first tile in the dashboard is an image tile of a fictitious waste utility, "Wide World Waste." You can customize the tile and put in your own image, or you can remove it.
- **Waste bin image tile:** You can use image and content tiles to create a visual representation of the device that's being monitored, along with a description.
- **Fill level KPI tile:** This tile displays a value reported by a *fill level* sensor in a waste bin. Fill level and other sensors, like *odor meter* or *weight* in a waste bin, can be remotely monitored. An operator can take an action such as dispatching a trash collection truck.
- **Waste monitoring area map:** This tile uses Azure Maps, which you can configure directly in Azure IoT Central. The map tile displays device location. Try to hover

over the map and try the controls over the map, like zoom-in, zoom-out, or expand.

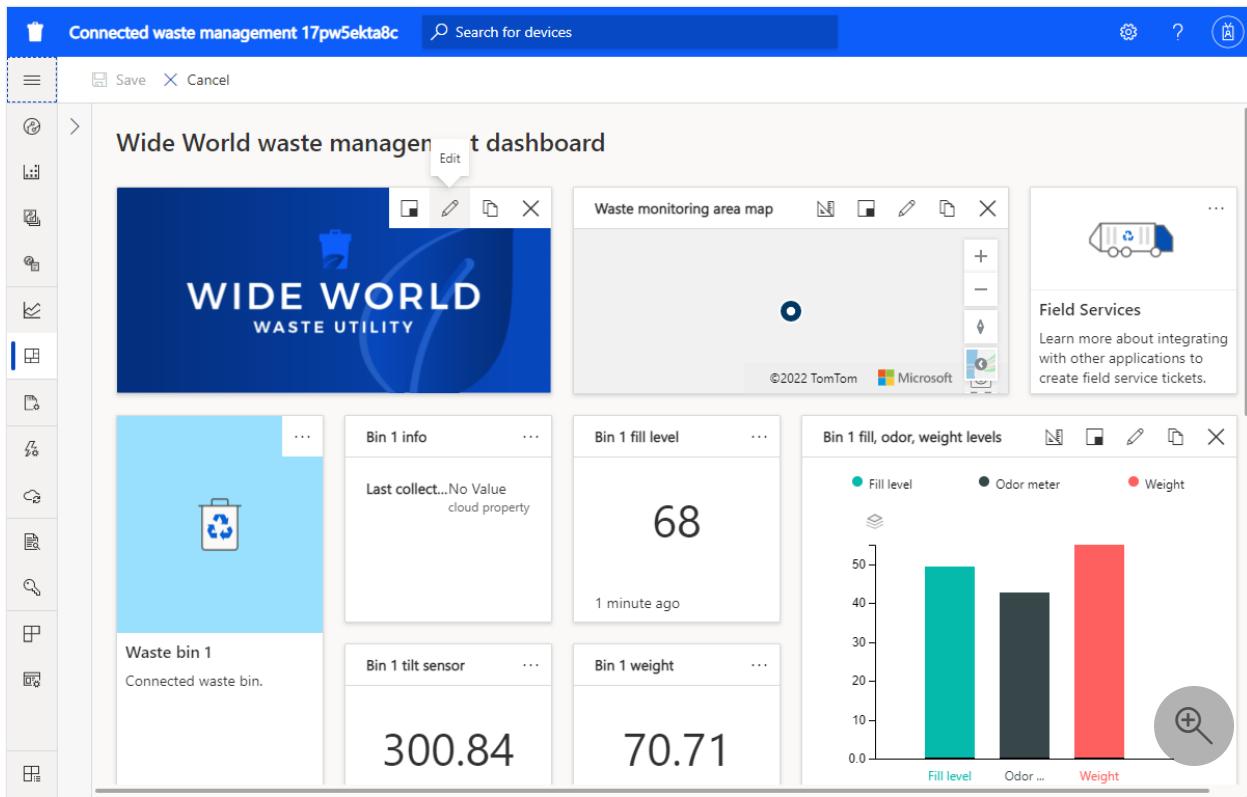
- **Fill, odor, weight level bar chart:** You can visualize one or multiple kinds of device telemetry data in a bar chart. You can also expand the bar chart.



- **Field Services:** The dashboard includes a link to "How to integrate with Dynamics 365 Field Services from your Azure IoT Central application." For example, you can use Field Services to create tickets for dispatching trash collection services.

Customize the dashboard

You can customize the dashboard by selecting the **Edit** menu. Then you can add new tiles or configure existing ones. Here's what the dashboard looks like in editing mode:



You can also select **+ New** to create a new dashboard and configure from scratch. You can have multiple dashboards, and you can switch between your dashboards from the dashboard menu.

Explore the device template

A device template in Azure IoT Central defines the capabilities of a device, which can include telemetry, properties, or commands. As a builder, you can define device templates that represent the capabilities of the devices you will connect.

The connected waste management application comes with a sample template for a connected waste bin device.

To view the device template:

1. In Azure IoT Central, from the left pane of your app, select **Device templates**.
2. In the **Device templates** list, select **Connected Waste Bin**.
3. Examine the device template capabilities. You can see that it defines sensors like **Fill level**, **Odor meter**, **Weight**, and **Location**.

Display name	Name *	Capability type *	Semantic type
Fill level	FillLevel	Telemetry	None
Weight	Weight	Telemetry	None
Location	Location	Property	Location
Odor meter	OdorMeter	Telemetry	None
Bin type	BinType	Property	None
Bin state	BinState	Telemetry	State
Tilt sensor	TiltSensor	Telemetry	None

Customize the device template

Try to customize the following features:

1. From the device template menu, select **Customize**.
2. Find the **Odor meter** telemetry type.
3. Update the **Display name** of **Odor meter** to **Odor level**.
4. Try to update the unit of measurement, or set **Min value** and **Max value**.
5. Select **Save**.

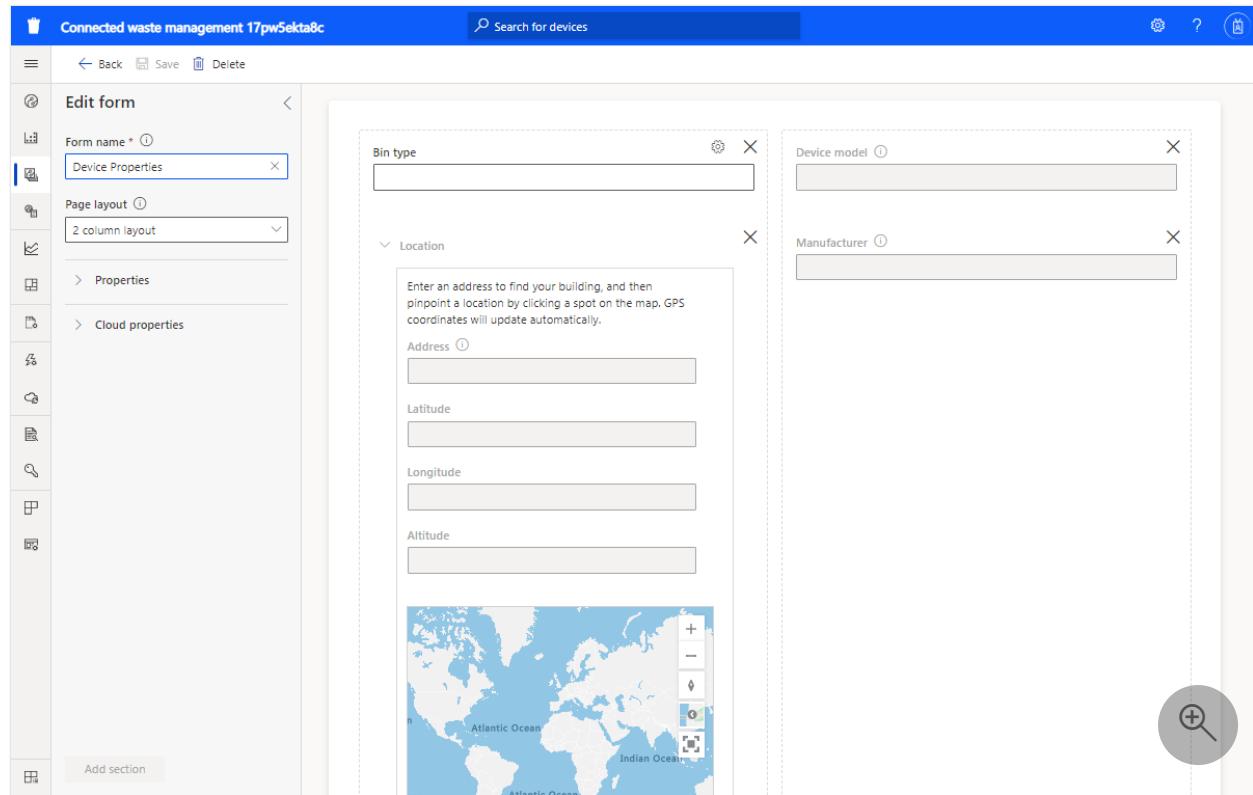
Add a cloud property

To add a cloud property:

1. Navigate to the **Connected Waste Bin** device template, and select **+ Add capability**.
2. Add a new cloud property by selecting **Cloud Property** as **Capability type**. In Azure IoT Central, you can add a property that is relevant to a device but that doesn't come from the device. For example, a cloud property might be an alerting threshold specific to installation area, asset information, or maintenance information.
3. Select **Save**.

Views

The connected waste bin device template comes with predefined views. Explore the views, and update them if you want to. The views define how operators see the device data and input cloud properties.



Publish

If you made any changes, remember to publish the device template.

Create a new device template

To create a new device template, select **+ New**, and follow the steps. You can create a custom device template from scratch, or you can choose a device template from the Azure device catalog.

Explore simulated devices

In Azure IoT Central, you can create simulated devices to test your device template and application.

The connected waste management application has two simulated devices associated with the connected waste bin device template.

View the devices

1. From the left pane of Azure IoT Central, select **Device**.

2. Select **Connected Waste Bin** device.

Explore the **Device Properties** and **Device Dashboard** tabs.

ⓘ Note

All the tabs have been configured from the device template views.

Add new devices

You can add new devices by selecting **+ New** on the **Devices** tab.

Explore and configure rules

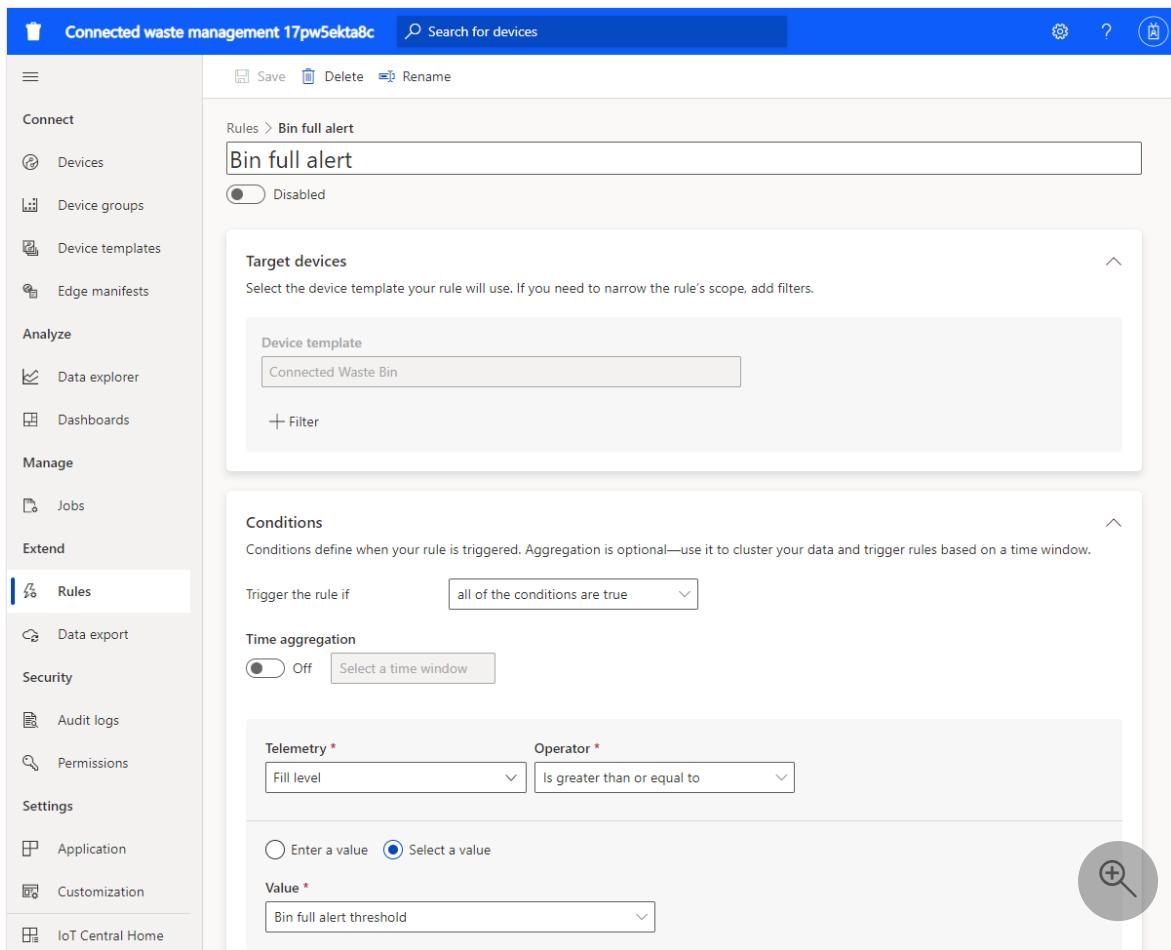
In Azure IoT Central, you can create rules to automatically monitor device telemetry, and to trigger actions when one or more conditions are met. The actions might include sending email notifications, triggering an action in Power Automate, or starting a webhook action to send data to other services.

The connected waste management application has four sample rules.

View rules

1. From the left pane of Azure IoT Central, select **Rules**.

2. Select Bin full alert.



Connected waste management 17pw5ekta8c

Rules > Bin full alert

Bin full alert

Disabled

Target devices

Select the device template your rule will use. If you need to narrow the rule's scope, add filters.

Device template: Connected Waste Bin

+ Filter

Conditions

Conditions define when your rule is triggered. Aggregation is optional—use it to cluster your data and trigger rules based on a time window.

Trigger the rule if: all of the conditions are true

Time aggregation: Off

Telemetry *: Fill level

Operator *: Is greater than or equal to

Value *: Bin full alert threshold

3. The **Bin full alert** checks the following condition: **Fill level is greater than or equal to Bin full alert threshold**.

The **Bin full alert threshold** is a cloud property that's defined in the connected waste bin device template.

Now create an email action.

Create an email action

In the **Actions** list of the rule, you can configure an email action:

1. Select **+** **Email**.
2. For **Display name**, enter **High pH alert**.
3. For **To**, enter the email address associated with your Azure IoT Central account.
4. Optionally, enter a note to include in the text of the email.
5. Select **Done > Save**.

You'll now receive an email when the configured condition is met.

Note

The application sends email each time a condition is met. Disable the rule to stop receiving email from the automated rule.

To create a new rule, from the left pane of **Rules**, select **+New**.

Configure jobs

In Azure IoT Central, jobs allow you to trigger device or cloud properties updates on multiple devices. You can also use jobs to trigger device commands on multiple devices. Azure IoT Central automates the workflow for you.

1. From the left pane of Azure IoT Central, select **Jobs**.
2. Select **+New**, and configure one or more jobs.

Customize your application

As an administrator, you can change settings to customize the user experience in your application.

Select **Customization > Appearance**, and then:

- To set the masthead logo image, select **Change**.
- To set the browser icon image that appears on browser tabs, select **Change**.
- Under **Browser colors**, you can replace the default browser colors by adding HTML hexadecimal color codes. For more information about color notation for HEX values, see the W3Schools [HTML Colors](#) tutorial.

You can change the application image on the **Application > Management** page.

Clean up resources

If you don't plan to continue using this application, you can delete it:

1. In your Azure IoT Central application, go to **Application > Management**.
2. Select **Delete**, and then confirm your action.

Next steps

[Connected water consumption concepts](#)

Azure for secure worldwide public sector cloud adoption

Article • 09/20/2022

Microsoft Azure is a multi-tenant cloud services platform that government agencies can use to deploy various solutions. A multi-tenant cloud platform implies that multiple customer applications and data are stored on the same physical hardware. Azure uses logical isolation to segregate each customer's applications and data. This approach provides the scale and economic benefits of multi-tenant cloud services while rigorously helping prevent customers from accessing one another's data or applications. Azure is available globally in more than 60 regions and can be used by government entities worldwide to meet rigorous data protection requirements across a broad spectrum of data classifications, including unclassified and classified data.

This article addresses common data residency, security, and isolation concerns pertinent to worldwide public sector customers. It also explores technologies available in Azure to safeguard both unclassified and classified workloads in the public multi-tenant cloud in combination with Azure Stack Hub and Azure Stack Edge deployed on-premises and at the edge.

Executive summary

Microsoft Azure provides strong customer commitments regarding data residency and transfer policies. Most Azure services enable you to specify the deployment region. For those services, Microsoft won't store your data outside your specified geography. You can use extensive and robust data encryption options to help safeguard your data in Azure and control who can access it.

Listed below are some of the options available to you to safeguard your data in Azure:

- You can choose to store your most sensitive content in services that store data at rest in Geography.
- You can obtain further protection by encrypting data with your own key using Azure Key Vault.
- While you can't control the precise network path for data in transit, data encryption in transit helps protect data from interception.
- Azure is a 24x7 globally operated service; however, support and troubleshooting rarely require access to your data.
- If you want extra control for support and troubleshooting scenarios, you can use Customer Lockbox for Azure to approve or deny access to your data.

- Microsoft will notify you of any breach of your data – customer or personal – within 72 hours of incident declaration.
- You can monitor potential threats and respond to incidents on your own using Microsoft Defender for Cloud.

Using Azure data protection technologies and intelligent edge capabilities from the Azure Stack portfolio of products, you can process confidential and secret data in secure isolated infrastructure within the public multi-tenant cloud or top secret data on premises and at the edge under your full operational control.

Introduction

Governments around the world are in the process of a digital transformation, actively investigating solutions and selecting architectures that will help them transition many of their workloads to the cloud. There are many drivers behind the digital transformation, including the need to engage citizens, empower employees, transform government services, and optimize government operations. Governments across the world are also looking to improve their cybersecurity posture to secure their assets and counter the evolving threat landscape.

For governments and the public sector industry worldwide, Microsoft provides [Azure](#) – a public multi-tenant cloud services platform – that you can use to deploy various solutions. A multi-tenant cloud services platform implies that multiple customer applications and data are stored on the same physical hardware. Azure uses [logical isolation](#) to segregate each customer's applications and data. This approach provides the scale and economic benefits of multi-tenant cloud services while rigorously helping prevent other customers from accessing your data or applications.

A hyperscale public cloud provides resiliency in time of natural disaster and warfare. The cloud provides capacity for failover redundancy and empowers sovereign nations with flexibility regarding global resiliency planning. Hyperscale public cloud also offers a feature-rich environment incorporating the latest cloud innovations such as artificial intelligence, machine learning, IoT services, intelligent edge, and many more to help government customers increase efficiency and unlock insights into their operations and performance.

Using Azure's public cloud capabilities, you benefit from rapid feature growth, resiliency, and the cost-effective operation of the hyperscale cloud while still obtaining the levels of isolation, security, and confidence required to handle workloads across a broad spectrum of data classifications, including unclassified and classified data. Using Azure data protection technologies and intelligent edge capabilities from the [Azure Stack](#) portfolio of products, you can process confidential and secret data in secure isolated

infrastructure within the public multi-tenant cloud or top secret data on-premises and at the edge under your full operational control.

This article addresses common data residency, security, and isolation concerns pertinent to worldwide public sector customers. It also explores technologies available in Azure to help safeguard unclassified, confidential, and secret workloads in the public multi-tenant cloud in combination with Azure Stack products deployed on-premises and at the edge for fully disconnected scenarios involving top secret data. Given that unclassified workloads comprise most scenarios involved in worldwide public sector digital transformation, Microsoft recommends that you start your cloud journey with unclassified workloads and then progress to classified workloads of increasing data sensitivity.

Data residency

Established privacy regulations are silent on **data residency and data location**, and permit data transfers in accordance with approved mechanisms such as the EU Standard Contractual Clauses (also known as EU Model Clauses). Microsoft commits contractually in the Microsoft Products and Services [Data Protection Addendum](#) (DPA) that all potential transfers of customer data out of the EU, European Economic Area (EEA), and Switzerland shall be governed by the EU Model Clauses. Microsoft will abide by the requirements of the EEA and Swiss data protection laws regarding the collection, use, transfer, retention, and other processing of personal data from the EEA and Switzerland. All transfers of personal data are subject to appropriate safeguards and documentation requirements. However, many customers considering cloud adoption are seeking assurances about customer and personal data being kept within the geographic boundaries corresponding to customer operations or location of customer's end users.

Data sovereignty implies data residency; however, it also introduces rules and requirements that define who has control over customer data stored in the cloud. In many cases, data sovereignty mandates that customer data be subject to the laws and legal jurisdiction of the country/region in which data resides. These laws can have direct implications on data access even for platform maintenance or customer-initiated support requests. You can use Azure public multi-tenant cloud in combination with Azure Stack products for on-premises and edge solutions to meet your data sovereignty requirements, as described later in this article. These other products can be deployed to put you solely in control of your data, including storage, processing, transmission, and remote access.

Among several [data categories and definitions](#) that Microsoft established for cloud services, the following four categories are discussed in this article:

- **Customer data** is all data that you provide to Microsoft to manage on your behalf through your use of Microsoft online services.
- **Customer content** is a subset of customer data and includes, for example, the content stored in your Azure Storage account.
- **Personal data** means any information associated with a specific natural person, for example, names and contact information of your end users. However, personal data could also include data that isn't customer data, such as user ID that Azure can generate and assign to your administrator – such personal data is considered pseudonymous because it can't identify an individual on its own.
- **Support and consulting data** mean all data provided by you to Microsoft to obtain support or Professional Services.

For more information about your options to control data residency and meet your data protection obligations, see [Enabling data residency and data protection in Microsoft Azure regions](#). The following sections address key cloud implications for data residency and the fundamental principles guiding Microsoft's safeguarding of your data at rest, in transit, and as part of support requests that you initiate.

Data at rest

Microsoft provides transparent insight into data location for all online services available to you from [Where your data is located](#). Expand *Cloud service data residency and transfer policies* section to reveal links for individual online services.

If you want to ensure your data is stored only in your chosen Geography, you should select from the many regional services that make this commitment.

Regional vs. non-regional services

Microsoft Azure provides [strong customer commitments](#) regarding data residency and transfer policies:

- **Data storage for regional services:** Most Azure services are deployed regionally and enable you to specify the region into which the service will be deployed. Microsoft won't store your data outside the Geography you specified except for a few regional services and Preview services as described on the Azure [data location page](#). This commitment helps ensure that your data stored in a given region will remain in the corresponding Geography, and won't be moved to another Geography for most regional services. For service availability, see [Products available by region](#).

- **Data storage for non-regional services:** Certain Azure services don't enable you to specify the region where the services will be deployed as described on the [data location page](#). For a complete list of non-regional services, see [Products available by region](#).

Your data in an Azure Storage account is [always replicated](#) to help ensure durability and high availability. Azure Storage copies your data to protect it from transient hardware failures, network or power outages, and even massive natural disasters. You can typically choose to replicate your data within the same data center, across availability zones within the same region, or across geographically separated regions. Specifically, when creating a storage account, you can select one of the following redundancy options:

- [Locally redundant storage \(LRS\)](#)
- [Zone-redundant storage \(ZRS\)](#)
- [Geo-redundant storage \(GRS\)](#)
- [Geo-zone-redundant storage \(GZRS\)](#)

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage provides LRS and ZRS redundancy options for replicating data in the primary region. For applications requiring high availability, you can choose geo-replication to a secondary region that is hundreds of kilometers away from the primary region. Azure Storage offers GRS and GZRS options for copying data to a secondary region. More options are available to you for configuring read access (RA) to the secondary region (RA-GRS and RA-GZRS), as explained in [Read access to data in the secondary region](#).

Azure Storage redundancy options can have implications on data residency as Azure relies on [paired regions](#) to deliver [geo-redundant storage](#) (GRS). For example, if you're concerned about geo-replication across regions that span country boundaries, you may want to choose LRS or ZRS to keep Azure Storage data at rest within the geographic boundaries of the country in which the primary region is located. Similarly, [geo replication for Azure SQL Database](#) can be obtained by configuring asynchronous replication of transactions to any region in the world, although it's recommended that paired regions be used for this purpose as well. If you need to keep relational data inside the geographic boundaries of your country/region, you shouldn't configure Azure SQL Database asynchronous replication to a region outside that country/region.

As described on the [data location page](#), most Azure **regional** services honor the data at rest commitment to ensure that your data remains within the geographic boundary where the corresponding service is deployed. A handful of exceptions to this rule are noted on the data location page. You should review these exceptions to determine if the type of data stored outside your chosen deployment Geography meets your needs.

Non-regional Azure services don't enable you to specify the region where the services will be deployed. Some non-regional services don't store your data at all but merely provide global routing functions such as Azure Traffic Manager or Azure DNS. Other non-regional services are intended for data caching at edge locations around the globe, such as the Content Delivery Network – such services are optional and you shouldn't use them for sensitive customer content you wish to keep in your Geography. One non-regional service that warrants extra discussion is **Microsoft Entra ID**, which is discussed in the next section.

Customer data in Microsoft Entra ID

Microsoft Entra ID is a non-regional service that may store identity data globally, except for Microsoft Entra deployments in:

- The United States, where identity data is stored solely in the United States.
- Europe, where Microsoft Entra ID keeps most of the identity data within European datacenters except as noted in [Identity data storage for European customers in Microsoft Entra ID](#).
- Australia and New Zealand, where identity data is stored in Australia except as noted in [Customer data storage for Australian and New Zealand customers in Microsoft Entra ID](#).

Microsoft Entra ID provides a [dashboard](#) with transparent insight into data location for every Microsoft Entra component service. Among other features, Microsoft Entra ID is an identity management service that stores directory data for your Azure administrators, including user **personal data** categorized as **End User Identifiable Information (EUII)**, for example, names, email addresses, and so on. In Microsoft Entra ID, you can create User, Group, Device, Application, and other entities using various attribute types such as Integer, DateTime, Binary, String (limited to 256 characters), and so on. Microsoft Entra ID isn't intended to store your customer content and it isn't possible to store blobs, files, database records, and similar structures in Microsoft Entra ID. Moreover, Microsoft Entra ID isn't intended to be an identity management service for your external end users – [Azure AD B2C](#) should be used for that purpose.

Microsoft Entra ID implements extensive **data protection features**, including tenant isolation and access control, data encryption in transit, secrets encryption and management, disk level encryption, advanced cryptographic algorithms used by various Microsoft Entra components, data operational considerations for insider access, and more. Detailed information is available from a whitepaper [Active Directory Data Security Considerations](#).

Generating pseudonymous data for internal systems

Personal data is defined broadly. It includes not just customer data but also unique personal identifiers such as Probably Unique Identifier (PUID) and Globally Unique Identifier (GUID), the latter being often labeled as Universally Unique Identifier (UUID). These unique personal identifiers are *pseudonymous identifiers*. This type of information is generated automatically to track users who interact directly with Azure services, such as your administrators. For example, PUID is a random string generated programmatically via a combination of characters and digits to provide a high probability of uniqueness. Pseudonymous identifiers are stored in centralized internal Azure systems.

Whereas EUII represents data that could be used on its own to identify a user (for example, user name, display name, user principal name, or even user-specific IP address), pseudonymous identifiers are considered pseudonymous because they can't identify an individual on their own. Pseudonymous identifiers don't contain any information that you uploaded or created.

Data in transit

While you can't control the precise network path for data in transit, data encryption in transit helps protect data from interception.

Data in transit applies to the following scenarios involving data traveling between:

- Your end users and Azure service
- Your on-premises datacenter and Azure region
- Microsoft datacenters as part of expected Azure service operation

While data in transit between two points within your chosen Geography will typically remain in that Geography, it isn't possible to guarantee this outcome 100% of the time because of the way networks automatically reroute traffic to avoid congestion or bypass other interruptions. That said, data in transit can be protected through encryption as detailed below and in [*Data encryption in transit*](#) section.

Your end users connection to Azure service

Most customers will connect to Azure over the Internet, and the precise routing of network traffic will depend on the many network providers that contribute to Internet infrastructure. As stated in the Microsoft Products and Services [**Data Protection Addendum**](#) (DPA), Microsoft doesn't control or limit the regions from which you or your end users may access or move customer data. You can increase security by

enabling encryption in transit. For example, you can use [Azure Application Gateway](#) to configure end-to-end encryption of traffic. As described in [Data encryption in transit](#) section, Azure uses the Transport Layer Security (TLS) protocol to help protect data when it's traveling between you and Azure services. However, Microsoft can't control network traffic paths corresponding to your end-user interaction with Azure.

Your datacenter connection to Azure region

[Virtual Network](#) (VNet) provides a means for Azure virtual machines (VMs) to act as part of your internal (on-premises) network. You have options to securely connect to a VNet from your on-premises infrastructure – choose an [IPSec protected VPN](#) (for example, point-to-site VPN or site-to-site VPN) or a private connection by using [Azure ExpressRoute](#) with several [data encryption options](#).

- **IPSec protected VPN** uses an encrypted tunnel established across the public Internet, which means that you need to rely on the local Internet service providers for any network-related assurances.
- **ExpressRoute** allows you to create private connections between Microsoft datacenters and your on-premises infrastructure or colocation facility. ExpressRoute connections don't go over the public Internet and offer lower latency and higher reliability than IPSec protected VPN connections. [ExpressRoute locations](#) are the entry points to Microsoft's global network backbone and they may or may not match the location of Azure regions. For example, you can connect to Microsoft in Amsterdam through ExpressRoute and have access to all Azure cloud services hosted in Northern and Western Europe. However, it's also possible to have access to the same Azure regions from ExpressRoute connections located elsewhere in the world. Once the network traffic enters the Microsoft backbone, it's guaranteed to traverse that private networking infrastructure instead of the public Internet.

Traffic across Microsoft global network backbone

As described in [Data at rest](#) section, Azure services such as Storage and SQL Database can be configured for geo-replication to help ensure durability and high availability especially for disaster recovery scenarios. Azure relies on [paired regions](#) to deliver [geo-redundant storage](#) (GRS), and paired regions are also recommended when configuring active [geo-replication](#) for Azure SQL Database. Paired regions are located within the same Geography.

Inter-region traffic is encrypted using [Media Access Control Security](#) (MACsec), which protects network traffic at the data link layer (Layer 2 of the networking stack) and relies

on AES-128 block cipher for encryption. This traffic stays entirely within the Microsoft [global network backbone](#) and never enters the public Internet. The backbone is one of the largest in the world with more than 200,000 km of lit fiber optic and undersea cable systems. However, network traffic isn't guaranteed to always follow the same path from one Azure region to another. To provide the reliability needed for the Azure cloud, Microsoft has many physical networking paths with automatic routing around congestion or failures for optimal reliability. Therefore, Microsoft can't guarantee that network traffic traversing between Azure regions will always be confined to the corresponding Geography. In networking infrastructure disruptions, Microsoft can reroute the encrypted network traffic across its private backbone to ensure service availability and best possible performance.

Data for customer support and troubleshooting

Azure is a 24x7 globally operated service; however, support and troubleshooting rarely requires access to your data. If you want extra control over support and troubleshooting scenarios, you can use [Customer Lockbox for Azure](#) to approve or deny access requests to your data.

Microsoft [Azure support](#) is available in markets where Azure is offered. It's staffed globally to accommodate 24x7 access to support engineers via email and phone for technical support. You can [create and manage support requests](#) in the Azure portal. As needed, frontline support engineers can escalate your requests to Azure DevOps personnel responsible for Azure service development and operations. These Azure DevOps engineers are also staffed globally. The same production access controls and processes are imposed on all Microsoft engineers, which include support staff comprised of both Microsoft full-time employees and subprocessors/vendors.

As explained in [Data encryption at rest](#) section, **your data is encrypted at rest** by default when stored in Azure and you can control your own encryption keys in Azure Key Vault. Moreover, access to your data isn't needed to resolve most customer support requests. Microsoft engineers rely heavily on logs to provide customer support. As described in [Insider data access](#) section, Azure has controls in place to restrict access to your data for support and troubleshooting scenarios should that access be necessary. For example, **Just-in-Time (JIT)** access provisions restrict access to production systems to Microsoft engineers who are authorized to be in that role and were granted temporary access credentials. As part of the support workflow, **Customer Lockbox** puts you in charge of approving or denying access to your data by Microsoft engineers. When combined, these Azure technologies and processes (data encryption, JIT, and Customer Lockbox) provide appropriate risk mitigation to safeguard confidentiality and integrity of your data.

Government customers worldwide expect to be fully in control of protecting their data in the cloud. As described in the next section, Azure provides extensive options for data encryption through its entire lifecycle (at rest, in transit, and in use), including customer control of encryption keys.

Data encryption

Azure has extensive support to safeguard your data using [data encryption](#). If you require extra security for your most sensitive customer content stored in Azure services, you can encrypt it using your own encryption keys that you control in Azure Key Vault. While you can't control the precise network path for data in transit, data encryption in transit helps protect data from interception. Azure supports the following data encryption models:

- Server-side encryption that uses service-managed keys, customer-managed keys (CMK) in Azure, or CMK in customer-controlled hardware.
- Client-side encryption that enables you to manage and store keys on-premises or in another secure location.

Data encryption provides isolation assurances that are tied directly to encryption key access. Since Azure uses strong ciphers for data encryption, only entities with access to encryption keys can have access to data. Revoking or deleting encryption keys renders the corresponding data inaccessible.

Encryption key management

Proper protection and management of encryption keys is essential for data security.

[Azure Key Vault](#) is a cloud service for securely storing and managing secrets. The Key Vault service supports two resource types:

- [Vault](#) supports software-protected and hardware security module (HSM)-protected [secrets, keys, and certificates](#). Vaults provide a multi-tenant, low-cost, easy to deploy, zone-resilient (where available), and highly available key management solution suitable for most common cloud application scenarios. The corresponding HSMs have [FIPS 140 Level 2](#) validation.
- [Managed HSM](#) supports only HSM-protected cryptographic keys. It provides a single-tenant, fully managed, highly available, zone-resilient (where available) HSM as a service to store and manage your cryptographic keys. It's most suitable for applications and usage scenarios that handle high value keys. It also helps you meet the most stringent security, compliance, and regulatory requirements.

Managed HSM uses [FIPS 140 Level 3](#) validated HSMs to protect your cryptographic keys.

Key Vault enables you to store your encryption keys in hardware security modules (HSMs) that are FIPS 140 validated. With Azure 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 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.

Note

Azure Key Vault is designed, deployed, and operated such that Microsoft and its agents don't see or extract your cryptographic keys. For extra assurances, see [How does Azure Key Vault protect your keys?](#)

For more information, see [Azure Key Vault](#).

Data encryption in transit

Azure provides many options for [encrypting data in transit](#). Data encryption in transit isolates your network traffic from other traffic and helps protect data from interception. For more information, see [Data encryption in transit](#).

Data encryption at rest

Azure provides extensive options for [encrypting data at rest](#) to help you safeguard your data and meet your compliance needs using both Microsoft-managed encryption keys and customer-managed encryption keys. This process relies on multiple encryption keys and services such as Azure Key Vault and Microsoft Entra ID to ensure secure key access and centralized key management. For more information about Azure Storage encryption and Azure Disk encryption, see [Data encryption at rest](#).

Azure SQL Database provides [transparent data encryption](#) (TDE) at rest by [default](#). TDE performs real-time encryption and decryption operations on the data and log files. Database Encryption Key (DEK) is a symmetric key stored in the database boot record for availability during recovery. It's secured via a certificate stored in the master database of the server or an asymmetric key called TDE Protector stored under your control in [Azure Key Vault](#). Key Vault supports [bring your own key](#) (BYOK), which enables you to store the TDE Protector in Key Vault and control key management tasks including key permissions, rotation, deletion, enabling auditing/reporting on all TDE Protectors,

and so on. The key can be generated by the Key Vault, imported, or [transferred to the Key Vault from an on-premises HSM device](#). You can also use the [Always Encrypted](#) feature of Azure SQL Database, which is designed specifically to help protect sensitive data by allowing you to encrypt data inside your applications and [never reveal the encryption keys to the database engine](#). In this manner, Always Encrypted provides separation between those users who own the data (and can view it) and those users who manage the data (but should have no access).

Data encryption in use

Microsoft enables you to protect your data throughout its entire lifecycle: at rest, in transit, and in use. Azure confidential computing and Homomorphic encryption are two techniques that safeguard your data while it's processed in the cloud.

Azure confidential computing

[Azure confidential computing](#) is a set of data security capabilities that offers encryption of data while in use. This approach means that data can be processed in the cloud with the assurance that it's always under your control, even when data is in use while in memory during computations. Azure confidential computing supports different virtual machines for IaaS workloads:

- **Trusted launch VMs:** [Trusted launch](#) is available across [generation 2 VMs](#), bringing hardened security features – secure boot, virtual trusted platform module, and boot integrity monitoring – that protect against boot kits, rootkits, and kernel-level malware.
- **Confidential VMs with AMD SEV-SNP technology:** You can choose Azure VMs based on AMD EPYC 7003 series CPUs to lift and shift applications without requiring any code changes. These AMD EPYC CPUs use AMD [Secure Encrypted Virtualization – Secure Nested Paging](#) (SEV-SNP) technology to encrypt your entire virtual machine at runtime. The encryption keys used for VM encryption are generated and safeguarded by a dedicated secure processor on the EPYC CPU and can't be extracted by any external means. These Azure VMs are currently in Preview and available to select customers. For more information, see [Azure and AMD announce landmark in confidential computing evolution](#).
- **Confidential VMs with Intel SGX application enclaves:** You can choose Azure VMs based on [Intel Software Guard Extensions](#) (Intel SGX) technology that supports confidentiality in a granular manner down to the application level. With this approach, when data is in the clear, which is needed for efficient data processing in

memory, the data is protected inside a hardware-based [trusted execution environment](#) (TEE, also known as an enclave), as depicted in Figure 1. Intel SGX isolates a portion of physical memory to create an enclave where select code and data are protected from viewing or modification. TEE helps ensure that only the application designer has access to TEE data – access is denied to everyone else including Azure administrators. Moreover, TEE helps ensure that only authorized code is permitted to access data. If the code is altered or tampered with, the operations are denied, and the environment is disabled.

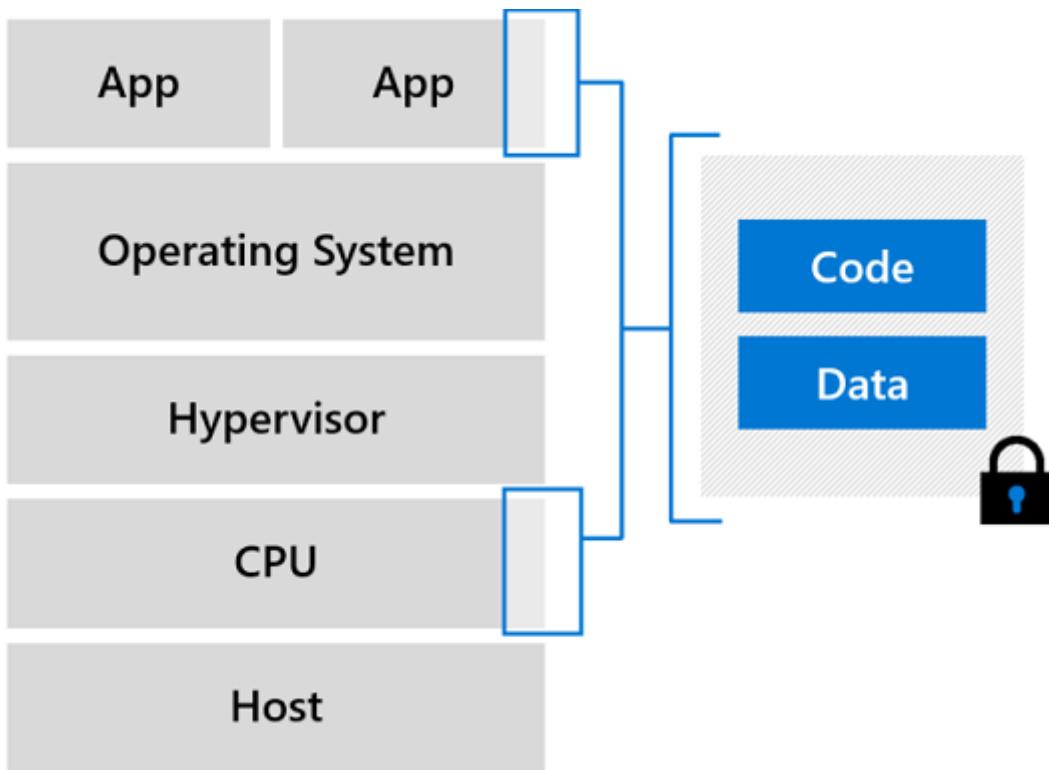


Figure 1. Trusted execution environment protection

Azure DCsv2, DCsv3, and DCdsv3 series virtual machines have the latest generation of Intel Xeon processors with Intel SGX technology. For more information, see [Build with SGX enclaves](#). The protection offered by Intel SGX, when used appropriately by application developers, can prevent compromise due to attacks from privileged software and many hardware-based attacks. An application using Intel SGX needs to be refactored into trusted and untrusted components. The untrusted part of the application sets up the enclave, which then allows the trusted part to run inside the enclave. No other code, irrespective of the privilege level, has access to the code executing within the enclave or the data associated with enclave code. Design best practices call for the trusted partition to contain just the minimum amount of content required to protect customer's secrets. For more information, see [Application development on Intel SGX](#).

Technologies like [Intel Software Guard Extensions](#) (Intel SGX), or [AMD Secure Encrypted Virtualization – Secure Nested Paging](#) (SEV-SNP) are recent CPU

improvements supporting confidential computing implementations. These technologies are designed as virtualization extensions and provide feature sets including memory encryption and integrity, CPU-state confidentiality and integrity, and attestation. Azure provides extra [Confidential computing offerings](#) that are generally available or available in preview:

- **Microsoft Azure Attestation** – A remote attestation service for validating the trustworthiness of multiple Trusted Execution Environments (TEEs) and verifying integrity of the binaries running inside the TEEs.
- **Azure Confidential Ledger** – A tamper-proof register for storing sensitive data for record keeping and auditing or for data transparency in multi-party scenarios. It offers Write-Once-Read-Many guarantees, which make data non-erasable and non-modifiable. The service is built on Microsoft Research's Confidential Consortium Framework.
- **Enclave aware containers** running on Azure Kubernetes Service (AKS) – Confidential computing nodes on AKS use Intel SGX to create isolated enclave environments in the nodes between each container application.
- **Always Encrypted with secure enclaves in Azure SQL** – The confidentiality of sensitive data is protected from malware and high-privileged unauthorized users by running SQL queries directly inside a TEE when the SQL statement contains any operations on encrypted data that require the use of the secure enclave where the database engine runs.
- **Confidential computing at the edge** – Azure IoT Edge supports confidential applications that run within secure enclaves on an Internet of Things (IoT) device. IoT devices are often exposed to tampering and forgery because they're physically accessible by bad actors. Confidential IoT Edge devices add trust and integrity at the edge by protecting the access to data captured by and stored inside the device itself before streaming it to the cloud.

Based on customer feedback, Microsoft has started to invest in higher-level [scenarios for Azure confidential computing](#). You can review the scenario recommendations as a starting point for developing your own applications using confidential computing services and frameworks.

Homomorphic encryption

[Homomorphic encryption](#)  refers to a special type of encryption technology that allows for computations to be performed on encrypted data, without requiring access to a key needed to decrypt the data. The results of the computation are encrypted and can be revealed only by the owner of the encryption key. In this manner, only the encrypted data are processed in the cloud and only you can reveal the results of the computation.

To help you adopt homomorphic encryption, [Microsoft SEAL](#) provides a set of encryption libraries that allow computations to be performed directly on encrypted data. This approach enables you to build end-to-end encrypted data storage and compute services where you never need to share your encryption keys with the cloud service. Microsoft SEAL aims to make homomorphic encryption easy to use and available to everyone. It provides a simple and convenient API and comes with several detailed examples demonstrating how the library can be used correctly and securely.

We also announced a [multi-year collaboration with Intel and the Defense Advanced Research Projects Agency \(DARPA\)](#) to lead the commercialization of fully homomorphic encryption (FHE). This technology will enable computation on always-encrypted data or cryptograms. With FHE, the data never needs to be decrypted, reducing the potential for cyber threats.

Data encryption in the cloud is an important risk mitigation requirement expected by government customers worldwide. As described in this section, Azure helps you protect your data through its entire lifecycle whether at rest, in transit, or even in use. Moreover, Azure offers comprehensive encryption key management to help you control your keys in the cloud, including key permissions, rotation, deletion, and so on. End-to-end data encryption using advanced ciphers is fundamental to ensuring confidentiality and integrity of your data in the cloud. However, many customers also expect assurances regarding any potential customer data access by Microsoft engineers for service maintenance, customer support, or other scenarios. These controls are described in the next section.

Insider data access

Insider threat is characterized as potential for providing back-door connections and cloud service provider (CSP) privileged administrator access to your systems and data. Microsoft provides strong [customer commitments](#) regarding who can access your data and on what terms. Access to your data by Microsoft operations and support personnel is **denied by default**. Access to your data isn't needed to operate Azure. Moreover, for most support scenarios involving customer-initiated troubleshooting tickets, access to your data isn't needed.

No default access rights and Just-in-Time (JIT) access provisions reduce greatly the risks associated with traditional on-premises administrator elevated access rights that typically persist throughout the duration of employment. Microsoft makes it considerably more difficult for malicious insiders to tamper with your applications and data. The same access control restrictions and processes are imposed on all Microsoft engineers, including both full-time employees and subprocessors/vendors.

For more information on how Microsoft restricts insider access to your data, see [Restrictions on insider access](#).

Government requests for your data

Government requests for your data follow a strict procedure according to [Microsoft practices for responding to government requests](#). Microsoft takes strong measures to help protect your data from inappropriate access or use by unauthorized persons. These measures include restricting access by Microsoft personnel and subcontractors and carefully defining requirements for responding to government requests for your data. Microsoft ensures that there are no back-door channels and no direct or unfettered government access to your data. Microsoft imposes special requirements for government and law enforcement requests for your data.

As stated in the Microsoft Products and Services [Data Protection Addendum](#) (DPA), Microsoft won't disclose your data to law enforcement unless required by law. If law enforcement contacts Microsoft with a demand for your data, Microsoft will attempt to redirect the law enforcement agency to request that data directly from you. If compelled to disclose your data to law enforcement, Microsoft will promptly notify you and provide a copy of the demand unless legally prohibited from doing so.

Government requests for your data must comply with applicable laws.

- A subpoena or its local equivalent is required to request non-content data.
- A warrant, court order, or its local equivalent is required for content data.

Every year, Microsoft rejects many law enforcement requests for your data. Challenges to government requests can take many forms. In many of these cases, Microsoft simply informs the requesting government that it's unable to disclose the requested information and explains the reason for rejecting the request. Where appropriate, Microsoft challenges requests in court.

Our [Law Enforcement Request Report](#) and [US National Security Order Report](#) are updated every six months and show that most of our customers are never impacted by government requests for data.

CLOUD Act provisions

The [CLOUD Act](#) is a United States law that was enacted in March 2018. For more information, see Microsoft's [blog post](#) and the [follow-up blog post](#) that describes Microsoft's call for principle-based international agreements governing law enforcement

access to data. Key points of interest to government customers procuring Azure services are captured below.

- The CLOUD Act enables governments to negotiate new government-to-government agreements that will result in greater transparency and certainty for how information is disclosed to law enforcement agencies across international borders.
- The CLOUD Act isn't a mechanism for greater government surveillance; it's a mechanism toward ensuring that your data is ultimately protected by the laws of your home country/region while continuing to facilitate lawful access to evidence for legitimate criminal investigations. Law enforcement in the US still needs to obtain a warrant demonstrating probable cause of a crime from an independent court before seeking the contents of communications. The CLOUD Act requires similar protections for other countries/regions seeking bilateral agreements.
- While the CLOUD Act creates new rights under new international agreements, it also preserves the common law right of cloud service providers to go to court to challenge search warrants when there's a conflict of laws – even without these new treaties in place.
- Microsoft retains the legal right to object to a law enforcement order in the United States where the order clearly conflicts with the laws of the country/region where your data is hosted. Microsoft will continue to carefully evaluate every law enforcement request and exercise its rights to protect customers where appropriate.
- For legitimate enterprise customers, US law enforcement will, in most instances, now go directly to customers rather than to Microsoft for information requests.

Microsoft doesn't disclose extra data as a result of the CLOUD Act. This law doesn't practically change any of the legal and privacy protections that previously applied to law enforcement requests for data – and those protections continue to apply. Microsoft adheres to the same principles and customer commitments related to government demands for user data.

Most government customers have requirements in place for handling security incidents, including data breach notifications. Microsoft has a mature security and privacy incident management process in place that is described in the next section.

Breach notifications

Microsoft will notify you of any breach of your data (customer or personal) within 72 hours of incident declaration. You can monitor potential threats and respond to incidents on your own using Microsoft Defender for Cloud.

Microsoft is responsible for monitoring and remediating security and availability incidents affecting the Azure platform and notifying you of any security breaches involving your data. Azure has a mature security and privacy incident management process that is used for this purpose. You're responsible for monitoring your own resources provisioned in Azure, as described in the next section.

Shared responsibility

The NIST [SP 800-145](#) standard defines the following cloud service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). The [shared responsibility](#) model for cloud computing is depicted in Figure 2. With on-premises deployment in your own datacenter, you assume the responsibility for all layers in the stack. As workloads get migrated to the cloud, Microsoft assumes progressively more responsibility depending on the cloud service model. For example, with the IaaS model, Microsoft's responsibility ends at the Hypervisor layer, and you're responsible for all layers above the virtualization layer, including maintaining the base operating system in guest Virtual Machines.

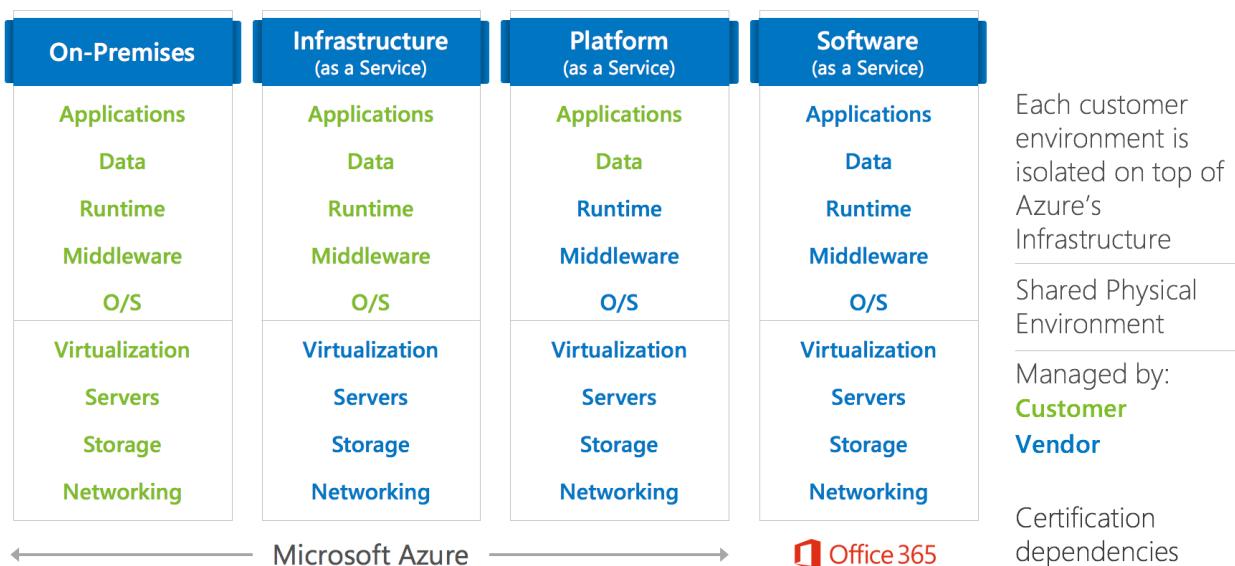


Figure 2. Shared responsibility model in cloud computing

In line with the shared responsibility model, Microsoft doesn't inspect, approve, or monitor your individual applications deployed on Azure. For example, Microsoft doesn't know what firewall ports need to be open for your application to function correctly, what the back-end database schema looks like, what constitutes normal network traffic for the application, and so on. Microsoft has extensive monitoring infrastructure in place for the cloud platform; however, you're responsible for provisioning and monitoring your own resources in Azure. You can deploy a range of Azure services to monitor and safeguard your applications and data, as described in the next section.

Essential Azure services for extra protection

Azure provides essential services that you can use to gain in-depth insight into your provisioned Azure resources and get alerted about suspicious activity, including outside attacks aimed at your applications and data. The [Azure Security Benchmark](#) provides security recommendations and implementation details to help you improve the security posture of your provisioned Azure resources.

For more information about essential Azure services for extra protection, see [Customer monitoring of Azure resources](#).

Breach notification process

Security incident response, including breach notification, is a subset of Microsoft's overall incident management plan for Azure. All Microsoft employees are trained to identify and escalate potential security incidents. A dedicated team of security engineers within the Microsoft Security Response Center (MSRC) is responsible for always managing the security incident response for Azure. Microsoft follows a five-step incident response process when managing both security and availability incidents for Azure services. The process includes the following stages:

1. Detect
2. Assess
3. Diagnose
4. Stabilize and recover
5. Close

The goal of this process is to restore normal service operations and security as quickly as possible after an issue is detected, and an investigation started. Moreover, Microsoft enables you to investigate, manage, and respond to security incidents in your Azure subscriptions. For more information, see [Incident management implementation guidance: Azure and Office 365](#).

If during the investigation of a security or privacy event, Microsoft becomes aware that customer or personal data has been exposed or accessed by an unauthorized party, the security incident manager is required to trigger the incident notification subprocess in consultation with the Microsoft legal affairs division. This subprocess is designed to fulfill incident notification requirements stipulated in Azure customer contracts (see *Security Incident Notification* in the Microsoft Products and Services [Data Protection Addendum](#)). Customer notification and external reporting obligations (if any) are triggered by a security incident being declared. The customer notification subprocess

begins in parallel with security incident investigation and mitigation phases to help minimize any impact resulting from the security incident.

Microsoft will notify you, Data Protection Authorities, and data subjects (each as applicable) of any breach of customer or personal data within 72 hours of incident declaration. **The notification process upon a declared security or privacy incident will occur as expeditiously as possible while still considering the security risks of proceeding quickly.** In practice, this approach means that most notifications will take place well before the 72-hr deadline to which Microsoft commits contractually.

Notification of a security or privacy incident will be delivered to one or more of your administrators by any means Microsoft selects, including via email. You should [provide security contact details](#) for your Azure subscription – this information will be used by Microsoft to contact you if the MSRC discovers that your data has been exposed or accessed by an unlawful or unauthorized party. To ensure that notification can be delivered successfully, it's your responsibility to maintain correct administrative contact information for each applicable subscription.

Most Azure security and privacy investigations don't result in declared security incidents. Most external threats don't lead to breaches of your data because of extensive platform security measures that Microsoft has in place. Microsoft has deployed extensive monitoring and diagnostics infrastructure throughout Azure that relies on big-data analytics and machine learning to get insight into the platform health, including real-time threat intelligence. While Microsoft takes all platform attacks seriously, it would be impractical to notify you of *potential* attacks at the platform level.

Aside from controls implemented by Microsoft to safeguard customer data, government customers deployed on Azure derive considerable benefits from security research that Microsoft conducts to protect the cloud platform. Microsoft global threat intelligence is one of the largest in the industry, and it's derived from one of the most diverse sets of threat telemetry sources. It's both the volume and diversity of threat telemetry that makes Microsoft machine learning algorithms applied to that telemetry so powerful. All Azure customers benefit directly from these investments as described in the next section.

Threat detection and prevention

The Microsoft [Graph Security API](#) uses advanced analytics to synthesize massive amounts of threat intelligence and security signals obtained across Microsoft products, services, and partners to combat cyberthreats. Millions of unique threat indicators across the most diverse set of sources are generated every day by Microsoft and its partners and shared across Microsoft products and services (Figure 3). Across its portfolio of

global services, each month Microsoft scans more than 400 billion email messages for phishing and malware, processes 450 billion authentications, executes more than 18 billion page scans, and scans more than 1.2 billion devices for threats. Importantly, this data always goes through strict privacy and compliance boundaries before being used for security analysis.

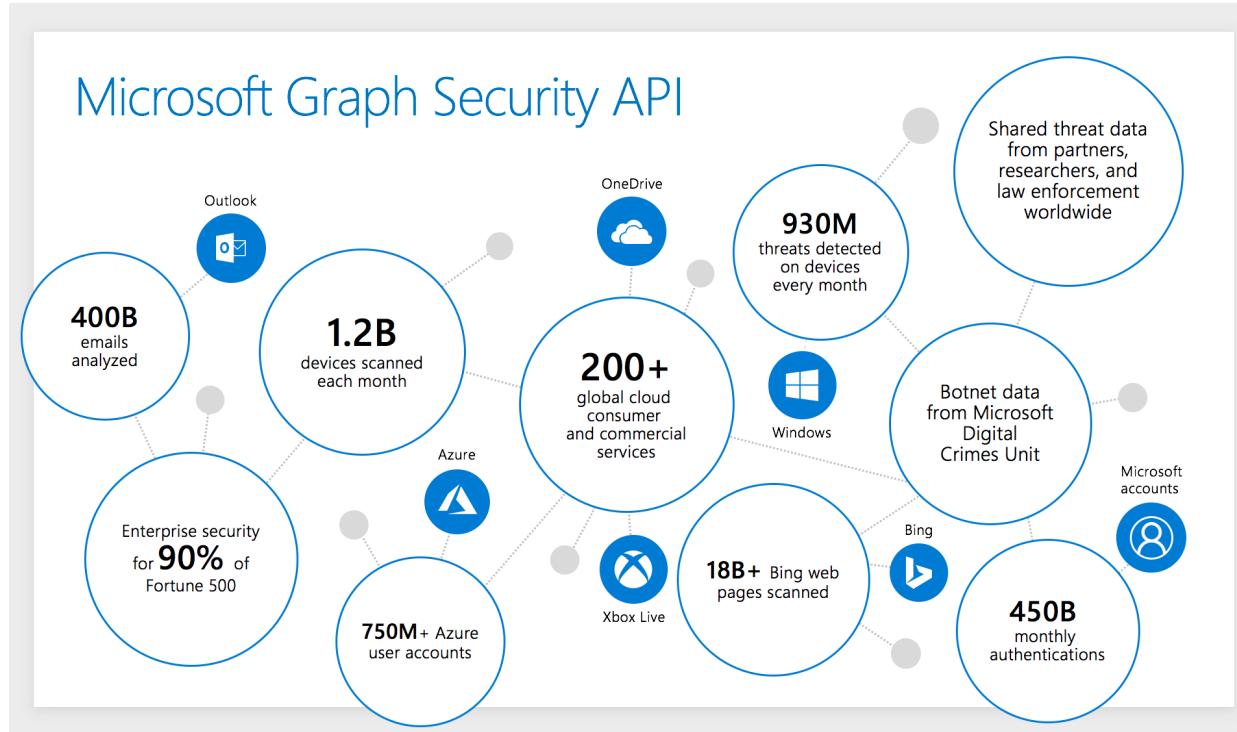


Figure 3. Microsoft global threat intelligence is one of the largest in the industry

The Microsoft Graph Security API provides an unparalleled view into the evolving threat landscape and enables rapid innovation to detect and respond to threats. Machine learning models and artificial intelligence reason over vast security signals to identify vulnerabilities and threats. The Microsoft Graph Security API provides a common gateway to [share and act on security insights](#) across the Microsoft platform and partner solutions. You benefit directly from the Microsoft Graph Security API as Microsoft makes the vast threat telemetry and advanced analytics [available in Microsoft online services](#), including Microsoft Defender for Cloud. These services can help you address your own security requirements in the cloud.

Microsoft has implemented extensive protections for the Azure cloud platform and made available a wide range of Azure services to help you monitor and protect your provisioned cloud resources from attacks. Nonetheless, for certain types of workloads and data classifications, government customers expect to have full operational control over their environment and even operate in a fully disconnected mode. The Azure Stack portfolio of products enables you to provision private and hybrid cloud deployment models that can accommodate highly sensitive data, as described in the next section.

Private and hybrid cloud with Azure Stack

Azure Stack [↗](#) portfolio is an extension of Azure that enables you to build and run hybrid applications across on-premises, edge locations, and cloud. As shown in Figure 4, Azure Stack includes Azure Stack Hyperconverged Infrastructure (HCI), Azure Stack Hub (formerly Azure Stack), and Azure Stack Edge (formerly Azure Data Box Edge). The last two components (Azure Stack Hub and Azure Stack Edge) are discussed in this section. For more information, see [Differences between global Azure, Azure Stack Hub, and Azure Stack HCI](#).

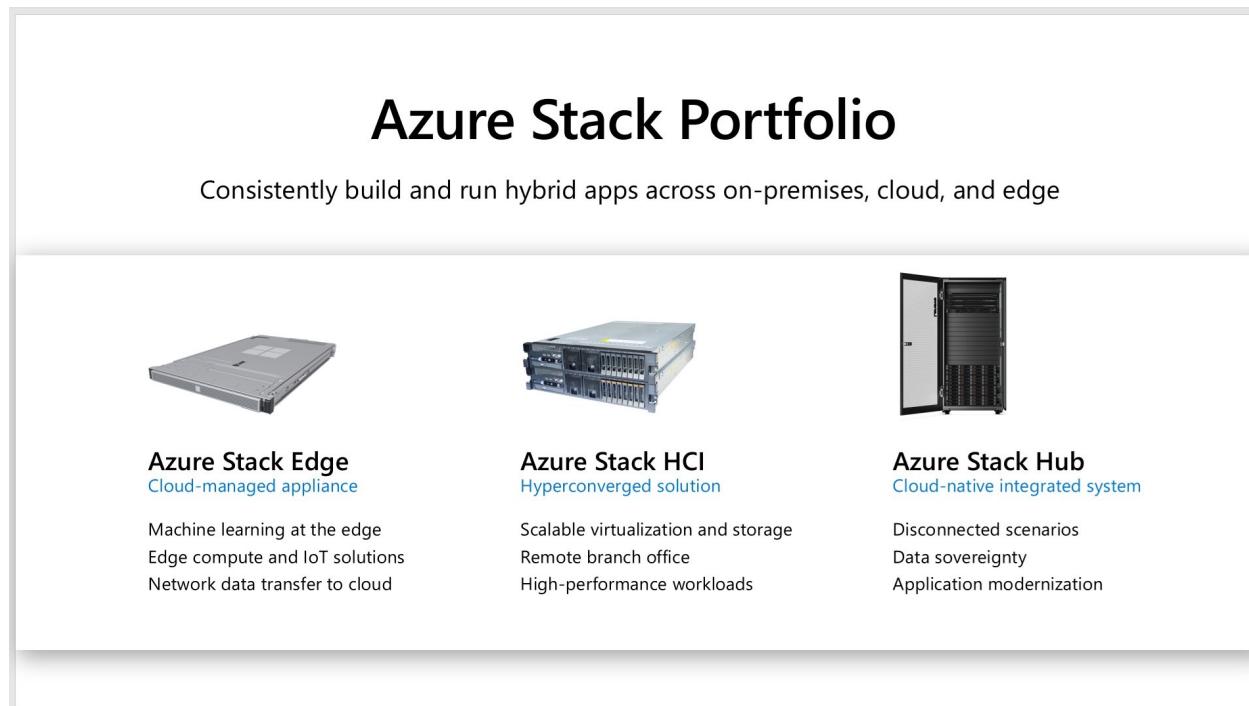


Figure 4. Azure Stack portfolio

Azure Stack Hub and Azure Stack Edge represent key enabling technologies that allow you to process highly sensitive data using a private or hybrid cloud and pursue digital transformation using Microsoft [intelligent cloud and intelligent edge](#) [↗](#) approach. For many government customers, enforcing data sovereignty, addressing custom compliance requirements, and applying maximum available protection to highly sensitive data are the primary driving factors behind these efforts.

Azure Stack Hub

Azure Stack Hub [↗](#) (formerly Azure Stack) is an integrated system of software and validated hardware that you can purchase from Microsoft hardware partners, deploy in your own data center, and then operate entirely on your own or with the help from a managed service provider. With Azure Stack Hub, you're always fully in control of access to your data. Azure Stack Hub can accommodate up to [16 physical servers per Azure Stack Hub scale unit](#). It represents an extension of Azure, enabling you to provision

various IaaS and PaaS services and effectively bring multi-tenant cloud technology to on-premises and edge environments. You can run many types of VM instances, App Services, Containers (including Azure AI containers), Functions, Azure Monitor, Key Vault, Event Hubs, and other services while using the same development tools, APIs, and management processes you use in Azure. Azure Stack Hub isn't dependent on connectivity to Azure to run deployed applications and enable operations via local connectivity.

In addition to Azure Stack Hub, which is intended for on-premises deployment (for example, in a data center), a ruggedized and field-deployable version called [Tactical Azure Stack Hub](#) is also available to address tactical edge deployments for limited or no connectivity, fully mobile requirements, and harsh conditions requiring military specification solutions.

Azure Stack Hub can be [operated disconnected](#) from Azure or the Internet. You can run the next generation of AI-enabled hybrid applications where your data lives. For example, you can rely on Azure Stack Hub to bring a trained AI model to the edge and integrate it with your applications for low-latency intelligence, with no tool or process changes for local applications.

Azure and Azure Stack Hub can help you unlock new hybrid use cases for externally facing or internally deployed line-of-business application, including edge and disconnected scenarios, cloud applications intended to meet data sovereignty and compliance requirements, and cloud applications deployed on-premises in your data center. These use cases may include mobile scenarios or fixed deployments within highly secure data center facilities. Figure 5 shows Azure Stack Hub capabilities and key usage scenarios.

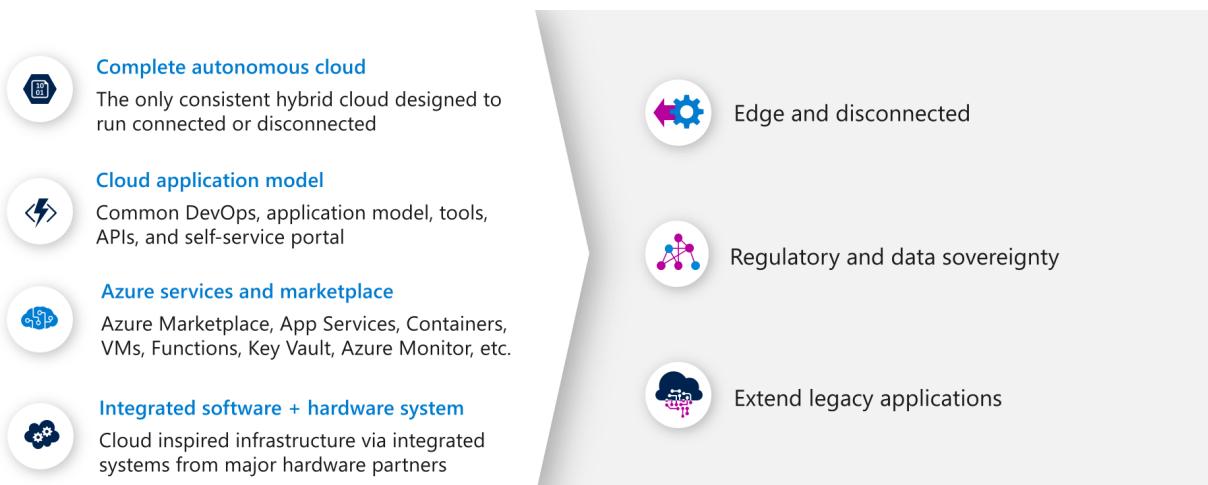


Figure 5. Azure Stack Hub capabilities

Azure Stack Hub brings the following [value proposition for key scenarios](#) shown in Figure 5:

- **Edge and disconnected solutions:** Address latency and connectivity requirements by processing data locally in Azure Stack Hub and then aggregating in Azure for further analytics, with common application logic across both (connected or disconnected). Aircraft, ship, or truck-delivered, Azure Stack Hub meets the tough demands of exploration, construction, agriculture, oil and gas, manufacturing, disaster response, government, and military efforts in the most extreme conditions and remote locations. For example, with Azure Stack Hub architecture for [edge and disconnected solutions](#), you can bring the next generation of AI-enabled hybrid applications to the edge where the data lives and integrate it with existing applications for low-latency intelligence.
- **Cloud applications to meet data sovereignty:** Deploy a single application differently depending on the country/region. You can develop and deploy applications in Azure, with full flexibility to deploy on-premises with Azure Stack Hub based on the need to meet data sovereignty or custom compliance requirements. For example, with Azure Stack Hub architecture for [data sovereignty](#), you can transmit data from an Azure VNet to Azure Stack Hub VNet over private connection and ultimately store data in a SQL Server database running in a VM on Azure Stack Hub. You can use Azure Stack Hub to accommodate even more restrictive requirements such as the need to deploy solutions in a disconnected environment managed by security-cleared, in-country/region personnel. These disconnected environments may not be permitted to connect to the Internet for any purpose because of the security classification they operate at.
- **Cloud application model on-premises:** Use Azure Stack Hub to update and extend legacy applications and make them cloud ready. With App Service on Azure Stack Hub, you can create a web front end to consume modern APIs with modern clients while taking advantage of consistent programming models and skills. For example, with Azure Stack Hub architecture for [legacy system modernization](#), you can apply a consistent DevOps process, Azure Web Apps, containers, serverless computing, and microservices architectures to modernize legacy applications while integrating and preserving legacy data in mainframe and core line-of-business systems.

Azure Stack Hub requires Microsoft Entra ID or Active Directory Federation Services (ADFS), backed by Active Directory as an [identity provider](#). You can use [role-based access control](#) (RBAC) to grant system access to authorized users, groups, and services by assigning them roles at a subscription, resource group, or individual resource level. Each role defines the access level a user, group, or service has over Azure Stack Hub resources.

Azure Stack Hub protects your data at the storage subsystem level using [encryption at rest](#). By default, Azure Stack Hub's storage subsystem is encrypted using BitLocker with 128-bit AES encryption. BitLocker keys are persisted in an internal secret store. At

deployment time, it's also possible to configure BitLocker to use 256-bit AES encryption. You can store and manage your secrets including cryptographic keys using [Key Vault in Azure Stack Hub](#).

Azure Stack Edge

[Azure Stack Edge](#) (formerly Azure Data Box Edge) is an AI-enabled edge computing device with network data transfer capabilities. The latest generation of these devices relies on a built-in Graphical Processing Unit (GPU) to enable accelerated AI inferencing. Azure Stack Edge uses GPU hardware natively integrated into the appliance to run machine learning algorithms at the edge efficiently. The size and portability allow you to run Azure Stack Edge as close to your users, apps, and data as needed. Figure 6 shows Azure Stack Edge capabilities and key use cases.

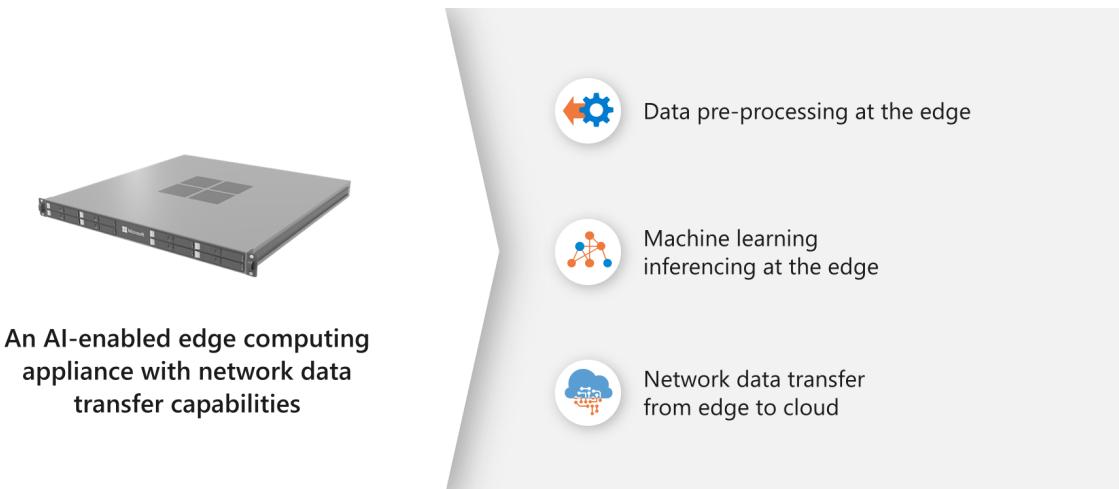


Figure 6. Azure Stack Edge capabilities

Azure Stack Edge brings the following [value proposition for key use cases](#) shown in Figure 6:

- **Inference with Azure Machine Learning:** Inference is a part of deep learning that takes place after model training, such as the prediction stage resulting from applying learned capability to new data. For example, it's the part that recognizes a vehicle in a target image after the model has been trained by processing many tagged vehicle images, often augmented by computer synthesized images (also known as synthetics). With Azure Stack Edge, you can run Machine Learning (ML) models to get results quickly and act on them before the data is sent to the cloud. The necessary subset of data (if there are bandwidth constraints) or the full data set is transferred to the cloud to continue to retrain and improve customer's ML models.
- **Preprocess data:** Analyze data from on-premises or IoT devices to quickly obtain results while staying close to where data is generated. Azure Stack Edge transfers the full data set (or just the necessary subset of data when bandwidth is an issue)

to the cloud to perform more advanced processing or deeper analytics.

Preprocessing can be used to aggregate data, modify data (for example, remove personally identifiable information or other sensitive data), transfer data needed for deeper analytics in the cloud, and analyze and react to IoT events.

- **Transfer data over network to Azure:** Use Azure Stack Edge to transfer data to Azure to enable further compute and analytics or for archival purposes.

Being able to gather, discern, and distribute mission data is essential for making critical decisions. Tools that help process and transfer data directly at the edge make this capability possible. For example, Azure Stack Edge, with its light footprint and built-in hardware acceleration for ML inferencing, is useful to further the intelligence of forward-operating units or similar mission needs with AI solutions designed for the tactical edge. Data transfer from the field, which is traditionally complex and slow, is made seamless with the [Azure Data Box](#) family of products.

These products unite the best of edge and cloud computing to unlock never-before-possible capabilities like synthetic mapping and ML model inferencing. From submarines to aircraft to remote bases, Azure Stack Hub and Azure Stack Edge allow you to harness the power of cloud at the edge.

Using Azure in combination with Azure Stack Hub and Azure Stack Edge, you can process confidential and sensitive data in a secure isolated infrastructure within the Azure public multi-tenant cloud or highly sensitive data at the edge under your full operational control. The next section describes a conceptual architecture for classified workloads.

Conceptual architecture

Figure 7 shows a conceptual architecture using products and services that support various data classifications. Azure public multi-tenant cloud is the underlying cloud platform that makes this architecture possible. You can augment Azure with on-premises and edge products such as Azure Stack Hub and Azure Stack Edge to accommodate critical workloads over which you seek increased or exclusive operational control. For example, Azure Stack Hub is intended for on-premises deployment in your data center where you have full control over service connectivity. Moreover, Azure Stack Hub can be deployed to address tactical edge deployments for limited or no connectivity, including fully mobile scenarios.

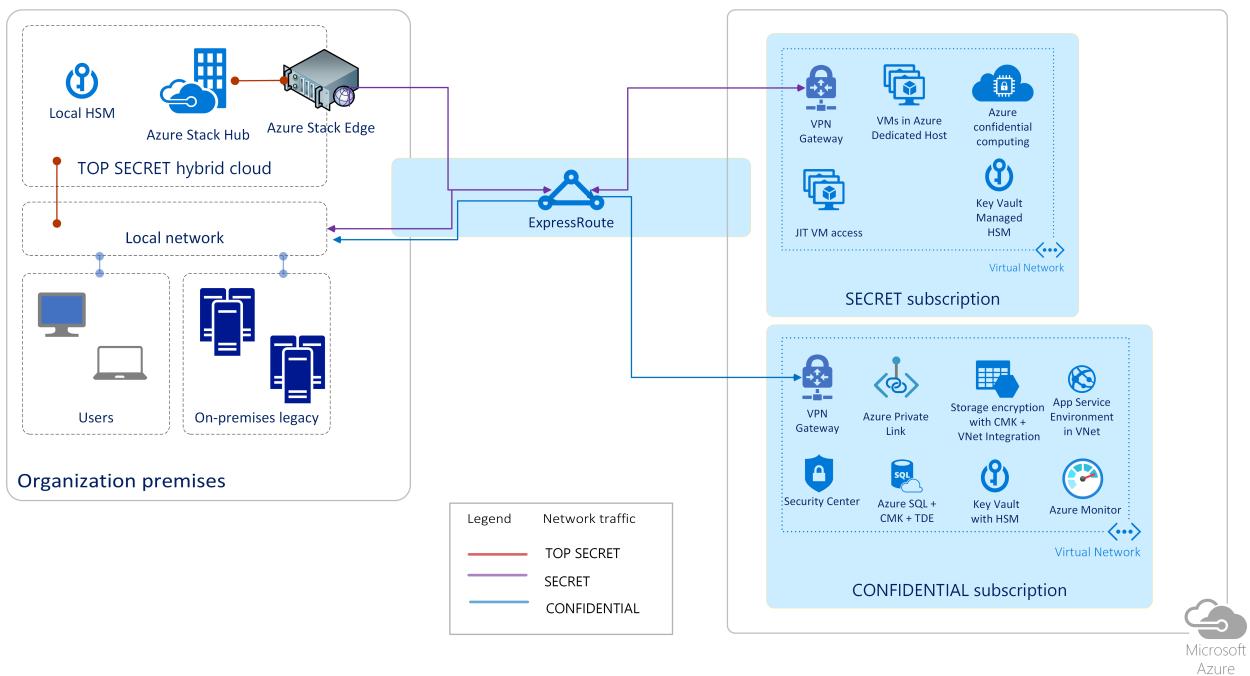


Figure 7. Conceptual architecture for classified workloads

For classified workloads, you can provision key enabling Azure services to secure target workloads while mitigating identified risks. Azure, in combination with [Azure Stack Hub](#) and [Azure Stack Edge](#), can accommodate private and hybrid cloud deployment models, making them suitable for many government workloads involving both unclassified and classified data. The following data classification taxonomy is used in this article:

- Confidential
- Secret
- Top secret

Similar data classification schemes exist in many countries/regions.

For top secret data, you can deploy Azure Stack Hub, which can operate disconnected from Azure and the Internet. [Tactical Azure Stack Hub](#) is also available to address tactical edge deployments for limited or no connectivity, fully mobile requirements, and harsh conditions requiring military specification solutions. Figure 8 depicts key enabling services that you can provision to accommodate various workloads on Azure.

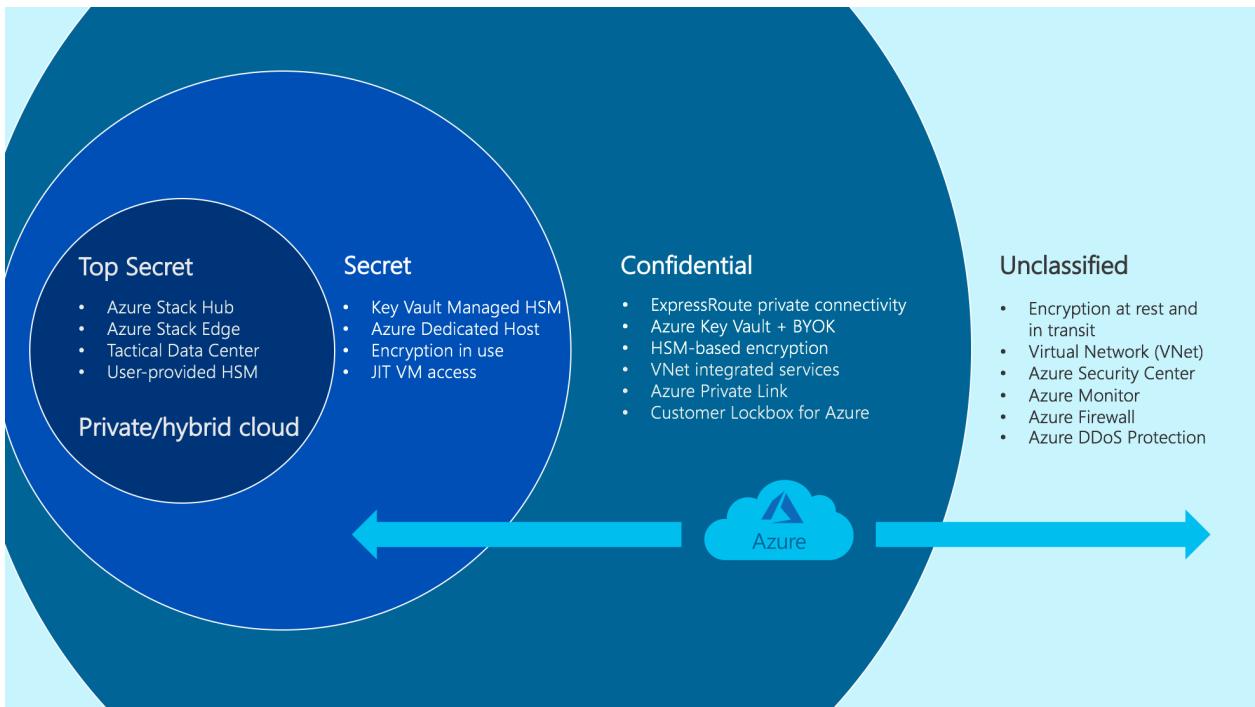


Figure 8. Azure support for various data classifications

Confidential data

Listed below are key enabling technologies and services that you may find helpful when deploying confidential data and workloads on Azure:

- All recommended technologies used for Unclassified data, especially services such as [Virtual Network](#) (VNet), [Microsoft Defender for Cloud](#), and [Azure Monitor](#).
- Public IP addresses are disabled allowing only traffic through private connections, including [ExpressRoute](#) and [Virtual Private Network](#) (VPN) gateway.
- Data encryption is recommended with customer-managed keys (CMK) in [Azure Key Vault](#) backed by multi-tenant hardware security modules (HSMs) that have FIPS 140 Level 2 validation.
- Only services that support [VNet integration](#) options are enabled. Azure VNet enables you to place Azure resources in a non-internet routable network, which can then be connected to your on-premises network using VPN technologies. VNet integration gives web apps access to resources in the virtual network.
- You can use [Azure Private Link](#) to access Azure PaaS services over a private endpoint in your VNet, ensuring that traffic between your VNet and the service travels across the Microsoft global backbone network, which eliminates the need to expose the service to the public Internet.
- [Customer Lockbox](#) for Azure enables you to approve/deny elevated access requests for your data in support scenarios. It's an extension of the Just-in-Time (JIT) workflow that comes with full audit logging enabled.

Using Azure public multi-tenant cloud capabilities, you can achieve the level of [isolation and security](#) required to store confidential data. You should use Microsoft Defender for Cloud and Azure Monitor to gain visibility into your Azure environments including the security posture of your subscriptions.

Secret data

Listed below are key enabling technologies and services that you may find helpful when deploying secret data and workloads on Azure:

- All recommended technologies used for confidential data.
- Use Azure Key Vault [Managed HSM](#), which provides a fully managed, highly available, single-tenant HSM as a service that uses FIPS 140 Level 3 validated HSMs. Each Managed HSM instance is bound to a separate security domain controlled by you and isolated cryptographically from instances belonging to other customers.
- [Azure Dedicated Host](#) provides physical servers that can host one or more Azure VMs and are dedicated to one Azure subscription. You can provision dedicated hosts within a region, availability zone, and fault domain. You can then place VMs directly into provisioned hosts using whatever configuration best meets your needs. Dedicated Host provides hardware isolation at the physical server level, enabling you to place your Azure VMs on an isolated and dedicated physical server that runs only your organization's workloads to meet corporate compliance requirements.
- Accelerated FPGA networking based on [Azure SmartNICs](#) enables you to offload host networking to dedicated hardware, enabling tunneling for VNets, security, and load balancing. Offloading network traffic to a dedicated chip guards against side-channel attacks on the main CPU.
- [Azure confidential computing](#) offers encryption of data while in use, ensuring that data is always under your control. Data is protected inside a hardware-based trusted execution environment (TEE, also known as enclave) and there's no way to view data or operations from outside the enclave.
- [Just-in-time \(JIT\) virtual machine \(VM\) access](#) can be used to lock down inbound traffic to Azure VMs by creating network security group (NSG) rules. You select ports on the VM to which inbound traffic will be locked down and when a user requests access to a VM, Microsoft Defender for Cloud checks that the user has proper role-based access control (RBAC) permissions.

To accommodate secret data in the Azure public multi-tenant cloud, you can deploy extra technologies and services on top of those technologies used for confidential data and limit provisioned services to those services that provide sufficient isolation. These

services offer various isolation options at run time. They also support data encryption at rest using customer-managed keys in single-tenant HSMs controlled by you and isolated cryptographically from HSM instances belonging to other customers.

Top secret data

Listed below are key enabling products that you may find helpful when deploying top secret data and workloads on Azure:

- All recommended technologies used for secret data.
- [Azure Stack Hub](#) (formerly Azure Stack) enables you to run workloads using the same architecture and APIs as in Azure while having a physically isolated network for your highest classification data.
- [Azure Stack Edge](#) (formerly Azure Data Box Edge) allows the storage and processing of highest classification data but also enables you to upload resulting information or models directly to Azure. This approach creates a path for information sharing between domains that makes it easier and more secure.
- In addition to Azure Stack Hub, which is intended for on-premises deployment (for example, in a data center), a ruggedized and field-deployable version called [Tactical Azure Stack Hub](#) is also available to address tactical edge deployments for limited or no connectivity, fully mobile requirements, and harsh conditions requiring military specification solutions.
- User-provided hardware security modules (HSMs) allow you to store your encryption keys in HSMs deployed on-premises and controlled solely by you.

Accommodating top secret data will likely require a disconnected environment, which is what Azure Stack Hub provides. Azure Stack Hub can be [operated disconnected](#) from Azure or the Internet. Even though “air-gapped” networks don't necessarily increase security, many governments may be reluctant to store data with this classification in an Internet connected environment.

Azure offers an unmatched variety of public, private, and hybrid cloud deployment models to address your concerns regarding the safeguarding of your data. The following section covers select use cases that might be of interest to worldwide government customers.

Select workloads and use cases

This section provides an overview of select use cases that showcase Azure capabilities for workloads that might be of interest to worldwide governments. In terms of

capabilities, Azure is presented via a combination of public multi-tenant cloud and on-premises + edge capabilities provided by [Azure Stack Hub](#) and [Azure Stack Edge](#).

Processing highly sensitive or regulated data on Azure Stack Hub

Microsoft provides Azure Stack Hub as an on-premises, cloud-consistent experience for customers who don't have the ability to connect directly to the Internet, or where certain workload types are required to be hosted in-country/region due to law, compliance, or sentiment. Azure Stack Hub offers IaaS and PaaS services and shares the same APIs as the global Azure cloud. Azure Stack Hub is available in scale units of 4, 8, and 16 servers in a single-server rack, and 4 servers in a military-specification, ruggedized set of transit cases, or multiple racks in a modular data center configuration.

Azure Stack Hub is a solution if you operate in scenarios where:

- For compliance reasons, you can't connect your network to the public Internet.
- For geo-political or security reasons, Microsoft can't offer connectivity to other Microsoft clouds.
- For geo-political or security reasons, the host organization may require cloud management by non-Microsoft entities, or in-country/region by security-cleared personnel.
- Microsoft doesn't have an in-country/region cloud presence and therefore can't meet data sovereignty requirements.
- Cloud management would pose significant risk to the physical well-being of Microsoft resources operating the environment.

For most of these scenarios, Microsoft and its partners offer a customer-managed, Azure Stack Hub-based private cloud appliance on field-deployable hardware from [major vendors](#) such as Avanade, Cisco, Dell EMC, Hewlett Packard Enterprise, and Lenovo. Azure Stack Hub is manufactured, configured, and deployed by the hardware vendor, and can be ruggedized and security-hardened to meet a broad range of environmental and compliance standards, including the ability to withstand transport by aircraft, ship, or truck, and deployment into colocation, mobile, or modular data centers. Azure Stack Hub can be used in exploration, construction, agriculture, oil and gas, manufacturing, disaster response, government, and military efforts in hospitable or the most extreme conditions and remote locations. Azure Stack Hub allows you the full autonomy to monitor, manage, and provision your own private cloud resources while meeting your connectivity, compliance, and ruggedization requirements.

Machine learning model training

Artificial intelligence (AI) holds tremendous potential for governments. Machine learning (ML) is a data science technique that allows computers to learn to use existing data, without being explicitly programmed, to forecast future behaviors, outcomes, and trends. Moreover, ML technologies can discover patterns, anomalies, and predictions that can help governments in their missions. As technical barriers continue to fall, decision-makers face the opportunity to develop and explore transformative AI applications. There are five main vectors that can make it easier, faster, and cheaper to adopt ML:

- Unsupervised learning
- Reducing need for training data
- Accelerated learning
- Transparency of outcome
- Deploying closer to where data lives

In the following sections, we expand on areas that can help you with some of the above vectors.

IoT analytics

In recent years, we have been witnessing massive proliferation of Internet of Things (IoT) devices and sensors. In almost all cases, these sensors gather signals and data from the environments and conditions they're designed for. The spectrum of capabilities for IoT sensors expands from measuring the level of moisture in soil all the way to gathering intelligence at 5,000-meters altitude. The high number of use cases imposes the necessity of applying data-analysis tools and procedures to realize value from the huge volumes of gathered data by IoT devices.

Governments are increasingly employing IoT devices for their missions, which could include maintenance predictions, borders monitoring, weather stations, smart meters, and field operations. In many cases, the data is often analyzed and inferred from where it's gathered. The main challenges of IoT analytics are: (1) large amount of data from independent sources, (2) analytics at the edge and often in disconnected scenarios, and (3) data and analysis aggregation.

With innovative solutions such as [IoT Hub](#) and [Azure Stack Edge](#), Azure services are well positioned to help you with these challenges.

Precision Agriculture with Farm Beats

Agriculture plays a vital role in most economies worldwide. In the US, over 70% of the rural households depend on agriculture as it contributes about 17% to the total GDP

and provides employment to over 60% of the population. In project [Farm Beats](#), we gather numerous data from farms that we couldn't get before, and then by applying AI and ML algorithms we're able to turn this data into actionable insights for farmers. We call this technique data-driven farming. What we mean by data-driven farming is the ability to map every farm and overlay it with data. For example, what is the soil moisture level 15 cm below surface, what is the soil temperature 15 cm below surface, and so on. These maps can then enable techniques, such as Precision Agriculture, which has been shown to improve yield, reduce costs, and benefit the environment. Despite the fact the Precision Agriculture as a technique was proposed more than 30 years ago, it hasn't taken off. The biggest reason is the inability to capture numerous data from farms to accurately represent the conditions in the farm. Our goal as part of the Farm Beats project is to be able to accurately construct precision maps at a fraction of the cost.

Unleashing the power of analytics with synthetic data

Synthetic data is data that is artificially created rather than being generated by actual events. It's often created with the help of computer algorithms and it's used for a wide range of activities, including usage as test data for new products and tools, as well as for ML models validation and improvements. Synthetic data can meet specific needs or conditions that aren't available in existing real data. For governments, the nature of synthetic data removes many barriers and helps data scientists with privacy concerns, accelerated learning, and data volume reduction needed for the same outcome. The main benefits of synthetic data are:

- **Overcoming restrictions:** Real data may have usage constraints due to privacy rules or other regulations. Synthetic data can replicate all important statistical properties of real data without exposing real data.
- **Scarcity:** Providing data where real data doesn't exist for a given event.
- **Precision:** Synthetic data is perfectly labeled.
- **Quality:** The quality of synthetic data can be precisely measured to fit the mission conditions.

Synthetic data can exist in several forms, including text, audio, video, and hybrid.

Knowledge mining

The exponential growth of unstructured data gathering in recent years has created many analytical problems for government agencies. This problem intensifies when data sets come from diverse sources such as text, audio, video, imaging, and so on.

[Knowledge mining](#) is the process of discovering useful knowledge from a collection of diverse data sources. This widely used data mining technique is a process that includes

data preparation and selection, data cleansing, incorporation of prior knowledge on data sets, and interpretation of accurate solutions from the observed results. This process has proven to be useful for large volumes of data in different government agencies.

For instance, captured data from the field often includes documents, pamphlets, letters, spreadsheets, propaganda, videos, and audio files across many disparate structured and unstructured formats. Buried within the data are [actionable insights](#) that can enhance effective and timely response to crisis and drive decisions. The objective of knowledge mining is to enable decisions that are better, faster, and more humane by implementing proven commercial algorithm-based technologies.

Scenarios for confidential computing

Security is a key driver accelerating the adoption of cloud computing, but it's also a major concern when customers are moving sensitive IP and data to the cloud.

Microsoft Azure provides broad capabilities to secure data at rest and in transit, but sometimes the requirement is also to protect data from threats as it's being processed.

[Azure confidential computing](#) supports two different confidential VMs for data encryption while in use:

- VMs based on AMD EPYC 7003 series CPUs for lift and shift scenarios without requiring any application code changes. These AMD EPYC CPUs use AMD [Secure Encrypted Virtualization – Secure Nested Paging](#) (SEV-SNP) technology to encrypt your entire virtual machine at runtime. The encryption keys used for VM encryption are generated and safeguarded by a dedicated secure processor on the EPYC CPU and can't be extracted by any external means.
- VMs that provide a hardware-based trusted execution environment (TEE, also known as enclave) based on [Intel Software Guard Extensions](#) (Intel SGX) technology. The hardware provides a protected container by securing a portion of the processor and memory. Only authorized code is permitted to run and to access data, so code and data are protected against viewing and modification from outside of TEE.

Azure confidential computing can directly address scenarios involving data protection while in use. For example, consider the scenario where data coming from a public or unclassified source needs to be matched with data from a highly sensitive source. Azure confidential computing can enable that matching to occur in the public cloud while protecting the highly sensitive data from disclosure. This circumstance is common in highly sensitive national security and law enforcement scenarios.

A second scenario involves data coming from multiple sources that needs to be analyzed together, even though none of the sources have the authority to see the data. Each individual provider encrypts the data they provide and only within the TEE is that data decrypted. As such, no external party and even none of the providers can see the combined data set. This capability is valuable for secondary use of healthcare data.

If you're deploying the types of workloads discussed in this section, you may need assurances from Microsoft that the underlying cloud platform security controls for which Microsoft is responsible are operating effectively. To address the needs of customers across regulated markets worldwide, Azure maintains a comprehensive compliance portfolio based on formal third-party certifications and other types of assurances to help you meet your own compliance obligations.

Compliance and certifications

Azure has the broadest [compliance coverage](#) in the industry, including key independent certifications and attestations such as ISO 27001, ISO 27017, ISO 27018, ISO 22301, ISO 9001, ISO 20000-1, SOC 1/2/3, PCI DSS Level 1, PCI 3DS, HITRUST, CSA STAR Certification, CSA STAR Attestation, US FedRAMP High, Australia IRAP, Germany C5, Japan ISMAP, Korea K-ISMS, Singapore MTCS Level 3, Spain ENS High, UK G-Cloud and Cyber Essentials Plus, and many more. Azure compliance portfolio includes more than 100 compliance offerings spanning globally applicable certifications, US Government-specific programs, industry assurances, and country/region-specific offerings. You can use these offerings when addressing your own compliance obligations across regulated industries and markets worldwide.

When deploying applications that are subject to regulatory compliance obligations on Azure, customers often seek assurances that all cloud services comprising the solution are included in the cloud service provider's audit scope. Azure offers industry-leading depth of compliance coverage judged by the number of cloud services in audit scope for each Azure certification. You can build and deploy realistic applications and benefit from extensive compliance coverage provided by Azure independent third-party audits.

Azure Stack Hub also provides [compliance documentation](#) to help you integrate Azure Stack Hub into solutions that address regulated workloads. You can download the following Azure Stack Hub compliance documents:

- PCI DSS assessment report produced by a third-party Qualified Security Assessor (QSA).
- Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) assessment report, including Azure Stack Hub control mapping to CCM domains and controls.

- FedRAMP High System Security Plan (SSP) precompiled template to demonstrate how Azure Stack Hub addresses applicable controls, Customer Responsibility Matrix for the FedRAMP High baseline, and FedRAMP assessment report produced by an accredited third-party assessment organization (3PAO).

Azure Policy regulatory compliance built-in initiatives map to compliance domains and controls in key standards, including:

- [Australian Government ISM PROTECTED](#)
- [Canada Federal PBMM](#)
- [ISO/IEC 27001](#)
- [US Government FedRAMP High](#)
- And others

For more regulatory compliance built-in initiatives, see [Azure Policy samples](#).

Regulatory compliance in Azure Policy provides built-in initiative definitions to view a list of the 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 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.

Azure compliance and certification resources are intended to help you address your own compliance obligations with various standards and regulations. You may have an established cloud adoption mandate in your country/region and the corresponding regulation to facilitate cloud onboarding. Or you may still operate traditional on-premises datacenters and are in the process of formulating your cloud adoption strategy. Azure's extensive compliance portfolio can help you irrespective of your cloud adoption maturity level.

Frequently asked questions

This section addresses common customer questions related to Azure public, private, and hybrid cloud deployment models.

Data residency and data sovereignty

- **Data location:** How does Microsoft keep data within a specific country/region's boundaries? In what cases does data leave? What data attributes leave? **Answer:** Microsoft provides [strong customer commitments](#) regarding cloud services data residency and transfer policies:
 - **Data storage for regional services:** Most Azure services are deployed regionally and enable you to specify the region into which the service will be deployed, for example, Europe. Microsoft won't store your data outside your specified Geography except for a few regional services and Preview services as described on the Azure [data location page](#). This commitment helps ensure that your data stored in a given region will remain in the corresponding Geography and won't be moved to another Geography for most regional services, including Storage, SQL Database, Virtual Machines, and many more.
 - **Data storage for non-regional services:** Certain Azure services don't enable you to specify the region where the services will be deployed as described on the [data location page](#). For a complete list of non-regional services, see [Products available by region](#).
- **Air-gapped (sovereign) cloud deployment:** Why doesn't Microsoft deploy an air-gapped, sovereign, physically isolated cloud instance in every country/region? **Answer:** Microsoft is actively pursuing air-gapped cloud deployments where a business case can be made with governments across the world. However, physical isolation or "air gapping", as a strategy, is diametrically opposed to the strategy of hyperscale cloud. The value proposition of the cloud, rapid feature growth, resiliency, and cost-effective operation, are diminished when the cloud is fragmented and physically isolated. These strategic challenges compound with each extra air-gapped cloud or fragmentation within an air-gapped cloud. Whereas an air-gapped cloud might prove to be the right solution for certain customers, it isn't the only available option.
- **Air-gapped (sovereign) cloud customer options:** How can Microsoft support governments who need to operate cloud services completely in-country/region by local security-cleared personnel? What options does Microsoft have for cloud services operated entirely on-premises within customer owned datacenter where government employees exercise sole operational and data access control? **Answer:** You can use [Azure Stack Hub](#) to deploy a private cloud on-premises managed by your own security-cleared, in-country/region personnel. You can run many types of VM instances, App Services, Containers (including Azure AI containers), Functions, Azure Monitor, Key Vault, Event Hubs, and other services while using the same development tools, APIs, and management processes that you use in Azure. With Azure Stack Hub, you have sole control of your data, including storage, processing, transmission, and remote access.

- **Local jurisdiction:** Is Microsoft subject to local country/region jurisdiction based on the availability of Azure public cloud service? **Answer:** Yes, Microsoft must comply with all applicable local laws; however, government requests for customer data must also comply with applicable laws. A subpoena or its local equivalent is required to request non-content data. A warrant, court order, or its local equivalent is required for content data. Government requests for customer data follow a strict procedure according to [Microsoft practices for responding to government requests](#). Every year, Microsoft rejects many law enforcement requests for customer data. Challenges to government requests can take many forms. In many of these cases, Microsoft simply informs the requesting government that it's unable to disclose the requested information and explains the reason for rejecting the request. Where appropriate, Microsoft challenges requests in court. Our [Law Enforcement Request Report](#) and [US National Security Order Report](#) are updated every six months and show that most of our customers are never impacted by government requests for data. For example, in the second half of 2019, Microsoft received 39 requests from law enforcement for accounts associated with enterprise cloud customers. Of those requests, only one warrant resulted in disclosure of customer content related to a non-US enterprise customer whose data was stored outside the United States.
- **Autarky:** Can Microsoft cloud operations be separated from the rest of Microsoft cloud and connected solely to local government network? Are operations possible without external connections to a third party? **Answer:** Yes, depending on the cloud deployment model.
 - **Public Cloud:** Azure regional datacenters can be connected to your local government network through dedicated private connections such as ExpressRoute. Independent operation without any connectivity to a third party such as Microsoft isn't possible in the public cloud.
 - **Private Cloud:** With Azure Stack Hub, you have full control over network connectivity and can operate Azure Stack Hub in [disconnected mode](#).
- **Data flow restrictions:** What provisions exist for approval and documentation of all data exchange between customer and Microsoft for local, in-country/region deployed cloud services? **Answer:** Options vary based on the cloud deployment model.
 - **Private cloud:** For private cloud deployment using Azure Stack Hub, you can control which data is exchanged with third parties. Azure Stack Hub telemetry can be turned off based on your preference and Azure Stack Hub can be operated disconnected. Moreover, Azure Stack Hub offers the [capacity-based billing model](#) in which no billing or consumption data leaves your on-premises infrastructure.

- **Public cloud:** In Azure public cloud, you can use [Network Watcher](#) to monitor network traffic associated with your workloads. For public cloud workloads, all billing data is generated through telemetry used exclusively for billing purposes and sent to Microsoft billing systems. You can [download and view](#) your billing and usage data; however, you can't prevent this information from being sent to Microsoft.
- **Patching and maintenance for private cloud:** How can Microsoft support patching and other maintenance for Azure Stack Hub private cloud deployment? **Answer:** Microsoft has a regular cadence in place for releasing [update packages for Azure Stack Hub](#). You're the sole operator of Azure Stack Hub and you can download and install these update packages. An update alert for Microsoft software updates and hotfixes will appear in the Update blade for Azure Stack Hub instances that are connected to the Internet. If your instance isn't connected and you would like to be notified about each update release, subscribe to the RSS or ATOM feed, as explained in our online documentation.

Safeguarding of customer data

- **Microsoft network security:** What network controls and security does Microsoft use? Can my requirements be considered? **Answer:** For insight into Azure infrastructure protection, you should review Azure [network architecture](#), Azure [production network](#), and Azure [infrastructure monitoring](#). If you're deploying Azure applications, you should review Azure [network security overview](#) and [network security best practices](#). To provide feedback or requirements, contact your Microsoft account representative.
- **Customer separation:** How does Microsoft logically or physically separate customers within its cloud environment? Is there an option for my organization to ensure complete physical separation? **Answer:** Azure uses [logical isolation](#) to separate your applications and data from other customers. This approach provides the scale and economic benefits of multi-tenant cloud services while rigorously enforcing controls designed to keep your data and applications off limits to other customers. There's also an option to enforce physical compute isolation via [Azure Dedicated Host](#), which provides physical servers that can host one or more Azure VMs and are dedicated to one Azure subscription. You can provision dedicated hosts within a region, availability zone, and fault domain. You can then place VMs directly into provisioned hosts using whatever configuration best meets your needs. Dedicated Host provides hardware isolation at the physical server level, enabling you to place your Azure VMs on an isolated and dedicated physical server that runs only your organization's workloads to meet corporate compliance requirements.

- **Data encryption at rest and in transit:** Does Microsoft enforce data encryption by default? Does Microsoft support customer-managed encryption keys? **Answer:** Yes, many Azure services, including Azure Storage and Azure SQL Database, encrypt data by default and support customer-managed keys. Azure [Storage encryption for data at rest](#) ensures that data is automatically encrypted before persisting it to Azure Storage and decrypted before retrieval. You can use [your own encryption keys](#) for Azure Storage encryption at rest and manage your keys in Azure Key Vault. Storage encryption is enabled by default for all new and existing storage accounts and it can't be disabled. When provisioning storage accounts, you can enforce "[secure transfer required](#)" option, which allows access only from secure connections. This option is enabled by default when creating a storage account in the Azure portal. Azure SQL Database enforces [data encryption in transit](#) by default and provides [transparent data encryption \(TDE\)](#) at rest [by default](#) allowing you to use Azure Key Vault and [bring your own key \(BYOK\)](#) functionality to control key management tasks including key permissions, rotation, deletion, and so on.
- **Data encryption during processing:** Can Microsoft protect my data while it's being processed in memory? **Answer:** Yes, [Azure confidential computing](#) supports two different technologies for data encryption while in use. First, you can use VMs based on Intel Xeon processors with [Intel Software Guard Extensions](#) (Intel SGX) technology. With this approach, data is protected inside a hardware-based trusted execution environment (TEE, also known as enclave), which is created by securing a portion of the processor and memory. Only authorized code is permitted to run and to access data, so application code and data are protected against viewing and modification from outside of TEE. Second, you can use VMs based on AMD EPYC 7003 series CPUs for lift and shift scenarios without requiring any application code changes. These AMD EPYC CPUs make it possible to encrypt your entire virtual machine at runtime. The encryption keys used for VM encryption are generated and safeguarded by a dedicated secure processor on the EPYC CPU and can't be extracted by any external means.
- **FIPS 140 validation:** Does Microsoft offer FIPS 140 Level 3 validated hardware security modules (HSMs) in Azure? If so, can I store AES-256 symmetric encryption keys in these HSMs? **Answer:** Azure Key Vault [Managed HSM](#) provides a fully managed, highly available, single-tenant HSM as a service that uses [FIPS 140 Level 3 validated HSMs](#). Each Managed HSM instance is bound to a separate security domain controlled by you and isolated cryptographically from instances belonging to other customers. With Managed HSMs, support is available for AES 128-bit and 256-bit symmetric keys.
- **Customer provided cryptography:** Can I use my own cryptography or encryption hardware? **Answer:** Yes, you can use your own HSMs deployed on-premises with your own crypto algorithms. However, if you expect to use customer-managed

keys for services integrated with [Azure Key Vault](#) (for example, Azure Storage, SQL Database, Disk encryption, and others), then you must use hardware security modules (HSMs) and [cryptography supported by Azure Key Vault](#).

- **Access to customer data by Microsoft personnel:** How does Microsoft restrict access to my data by Microsoft engineers? **Answer:** Microsoft engineers [don't have default access](#) to your data in the cloud. Instead, they can be granted access, under management oversight, only when necessary using a [restricted access workflow](#). Most customer support requests can be resolved without accessing your data as Microsoft engineers rely heavily on logs for troubleshooting and support. If a Microsoft engineer requires elevated access to your data as part of the support workflow, you can use [Customer Lockbox](#) for Azure to control how a Microsoft engineer accesses your data. Customer Lockbox for Azure puts you in charge of that decision by enabling you to approve/deny such elevated access requests. For more information on how Microsoft restricts insider access to your data, see [Restrictions on insider access](#).

Operations

- **Code review:** What can Microsoft do to prevent malicious code from being inserted into services that my organization uses? Can I review Microsoft code deployments? **Answer:** Microsoft has invested heavily in security assurance processes and practices to correctly develop logically isolated services and systems. For more information, see [Security assurance processes and practices](#). For more information about Azure Hypervisor isolation, see [Defense-in-depth exploit mitigations](#). Microsoft has full control over all source code that comprises Azure services. For example, the procedure for patching guest VMs differs greatly from traditional on-premises patching where patch verification is necessary following installation. In Azure, patches aren't applied to guest VMs; instead, the VM is simply restarted and when the VM boots, it's guaranteed to boot from a known good image that Microsoft controls. There's no way to insert malicious code into the image or interfere with the boot process. PaaS VMs offer more advanced protection against persistent malware infections than traditional physical server solutions, which if compromised by an attacker can be difficult to clean, even after the vulnerability is corrected. With PaaS VMs, reimaging is a routine part of operations, and it can help clean out intrusions that haven't even been detected. This approach makes it more difficult for a compromise to persist. You can't review Azure source code; however, online access to view source code is available for key products through the Microsoft [Government Security Program](#) (GSP).
- **DevOps personnel (cleared nationals):** What controls or clearance levels does Microsoft have for the personnel that have DevOps access to cloud environments

or physical access to data centers? **Answer:** Microsoft conducts [background screening](#) on operations personnel with access to production systems and physical data center infrastructure. Microsoft cloud background check includes verification of education and employment history upon hire, and extra checks conducted every two years thereafter (where permissible by law), including criminal history check, OFAC list, BIS denied persons list, and DDTC debarred parties list.

- **Data center site options:** Is Microsoft willing to deploy a data center to a specific physical location to meet more advanced security requirements? **Answer:** You should inquire with your Microsoft account team regarding options for data center locations.
- **Service availability guarantee:** How can my organization ensure that Microsoft (or particular government or other entity) can't turn off our cloud services? **Answer:** You should review the Microsoft [Product Terms](#) (formerly Online Services Terms) and the Microsoft Products and Services [Data Protection Addendum](#) (DPA) for contractual commitments Microsoft makes regarding service availability and use of online services.
- **Non-traditional cloud service needs:** What options does Microsoft provide for periodically internet free/disconnected environments? **Answer:** In addition to [Azure Stack Hub](#), which is intended for on-premises deployment and disconnected scenarios, a ruggedized and field-deployable version called [Tactical Azure Stack Hub](#) is also available to address tactical edge deployments for limited or no connectivity, fully mobile requirements, and harsh conditions requiring military specification solutions.

Transparency and audit

- **Audit documentation:** Does Microsoft make all audit documentation readily available to customers to download and examine? **Answer:** Yes, Microsoft makes independent third-party audit reports and other related documentation available for download under a non-disclosure agreement from the Azure portal. You'll need an existing Azure subscription or [free trial subscription](#) to access the Microsoft Defender for Cloud [audit reports blade](#). Extra compliance documentation is available from the Service Trust Portal (STP) [Audit Reports](#) section. You must log in to access audit reports on the STP. For more information, see [Get started with the Microsoft Service Trust Portal](#).
- **Process auditability:** Does Microsoft make its processes, data flow, and documentation available to customers or regulators for audit? **Answer:** Microsoft offers a Regulator Right to Examine, which is a program Microsoft implemented to provide regulators with direct right to examine Azure, including the ability to conduct an on-site examination, to meet with Microsoft personnel and Microsoft

external auditors, and to access any related information, records, reports, and documents.

- **Service documentation:** Can Microsoft provide in-depth documentation covering service architecture, software and hardware components, and data protocols?
Answer: Yes, Microsoft provides extensive and in-depth Azure online documentation covering all these topics. For example, you can review documentation on Azure [products, global infrastructure](#)  , and [API reference](#).

Next steps

Learn more about:

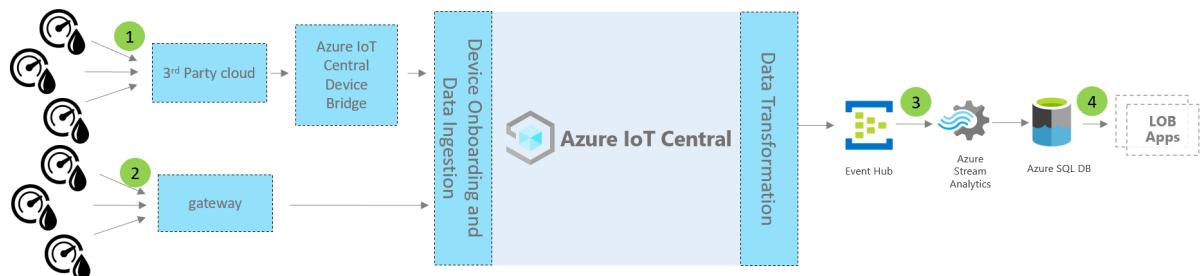
- [Azure Security](#)
- [Azure Compliance](#)
- [Azure compliance offerings](#)
- [Azure guidance for secure isolation](#)
- [Azure for government - worldwide government](#) 
- [Enabling data residency and data protection in Microsoft Azure regions](#) 
- [Azure Policy regulatory compliance samples](#)

Tutorial: Deploy and walk through the water consumption monitoring application

Article • 07/17/2023

Traditional water consumption tracking relies on water operators manually reading water consumption meters at the meter sites. More cities are replacing traditional meters with advanced smart meters enabling remote monitoring of consumption and remote control of valves that control water flow. Water consumption monitoring coupled with digital feedback messages to citizens can increase awareness and reduce water consumption.

The *water consumption monitoring* application template helps you kickstart your IoT solution development to enable water utilities to remotely monitor and control water flow.



Devices and connectivity (1,2)

Water management solutions use smart water devices such as flow meters, water quality monitors, smart valves, leak detectors.

Devices in smart water solutions may connect through low-power wide area networks or through a third-party network operator. For these types of devices, use the [Azure IoT Central Device Bridge](#) to send your device data to your IoT application in Azure IoT Central. You can also use an IP capable device gateway that connects directly to your IoT Central application.

IoT Central

When you build an IoT solution, Azure IoT Central simplifies the build process and helps to reduce the burden and costs of IoT management, operations, and development. You can brand, customize, and integrate your solution with third-party services.

When you connect your smart water devices to IoT Central, the application provides:

- Device command and control.
- Monitoring and alerting.
- A user interface with built-in role-based access controls.
- Configurable dashboards.
- Extensibility options.

Extensibility and integrations (3)

You can extend your IoT application in IoT Central and optionally:

- Transform and integrate your IoT data for advanced analytics through data export from your IoT Central application.
- Automate workflows in other systems by triggering actions using Power Automate or webhooks from IoT Central application.
- Programmatically access your IoT Central application by using the IoT Central REST APIs.

Business applications (4)

You can use IoT data to power various business applications within a water utility. In your IoT Central water consumption monitoring application you can configure rules and actions, and set them to create alerts in [Connected Field Service](#). Configure Power Automate in IoT Central rules to automate workflows across applications and services. Additionally, based on service activities in Connected Field Service, information can be sent back to Azure IoT Central.

In this tutorial, you learn how to:

- ✓ Use the Azure IoT Central water consumption monitoring template to create your water consumption monitoring application.
- ✓ Explore and customize the dashboard.
- ✓ Explore device templates.
- ✓ Explore simulated devices.
- ✓ Explore and configure rules.

- ✓ Configure jobs.
- ✓ Customize your application branding by using white labeling.

Prerequisites

An active Azure subscription. If you don't have an Azure subscription, create a [free account](#) before you begin.

Create water consumption monitoring application

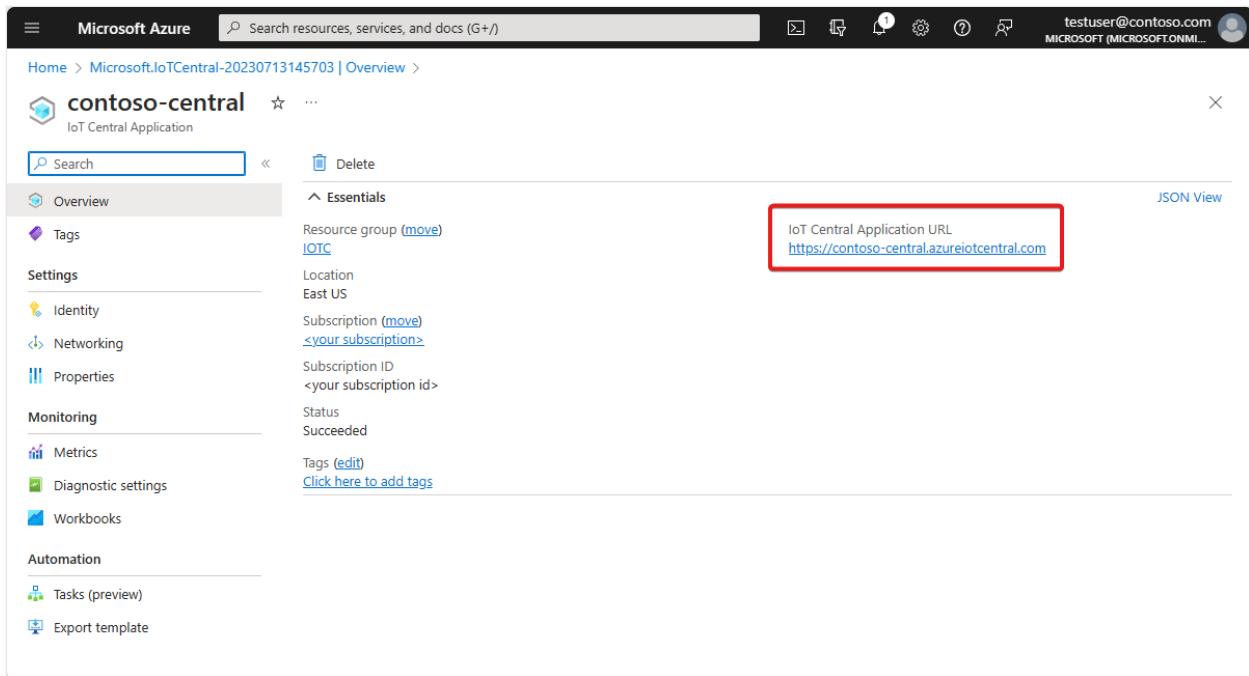
To create your IoT Central application:

1. Navigate to the [Create IoT Central Application](#) page in the Azure portal. If prompted, sign in with your Azure account.
2. Enter the following information:

Field	Description
Subscription	The Azure subscription you want to use.
Resource group	The resource group you want to use. You can create a new resource group or use an existing one.
Resource name	A valid Azure resource name.
Application URL	The URL subdomain for your application. The URL for an IoT Central application looks like <code>https://yoursubdomain.azureiotcentral.com</code> .
Template	Water Consumption Monitoring
Region	The Azure region you want to use.
Pricing plan	The pricing plan you want to use.

3. Select **Review + create**. Then select **Create**.

When the app is ready, you can navigate to it from the Azure portal:



contoso-central

IoT Central Application

Search

Delete

Overview

Tags

Settings

- Identity
- Networking
- Properties

Monitoring

- Metrics
- Diagnostic settings
- Workbooks

Automation

- Tasks (preview)
- Export template

Resource group (move)
IOTC

Location
East US

Subscription (move)
<your subscription>

Subscription ID
<your subscription id>

Status
Succeeded

Tags (edit)
Click here to add tags

IoT Central Application URL
<https://contoso-central.azureiotcentral.com>

JSON View

💡 Tip

To list all the IoT Central applications you have access to, navigate to [IoT Central Applications](#).

To learn more, see [Create an Azure IoT Central application](#).

Walk through the application

The following sections walk you through the key features of the application:

Dashboard

After you create the application, the sample **Wide World water consumption dashboard** opens.

You can create and customize views on the dashboard for operators.

Note

All data displayed on the dashboard is based on simulated device data, which you explore in the next section.

The dashboard consists of different kinds of tiles:

- **Wide World Water Utility image tile:** The first tile in the dashboard is an image tile of the fictitious water utility Wide World Water. You can customize the tile by inserting your own image or removing it.
- **Average water flow KPI tile:** The KPI tile is configured to display as an example *the average in the last 30 minutes*. You can customize the KPI tile and set it to a different type and time range.
- **Device command tiles:** These tiles include the **Close valve**, **Open valve**, and **Set valve position** tiles. Selecting the commands takes you to the simulated device command page. In Azure IoT Central, a *command* is a *device capability* type. You explore this concept later in the [Device template](#) section of this tutorial.
- **Water distribution area map:** The map uses Azure Maps, which you can configure directly in Azure IoT Central. The map tile displays the device location. Hover over

the map and try the controls over the map, like *zoom in*, *zoom out*, or *expand*.

- **Average water flow line chart and Environmental condition line chart:** You can visualize one or multiple device telemetries plotted as a line chart over a desired time range.
- **Average valve pressure heatmap chart:** You can choose the heatmap visualization type of device telemetry data you want to see distributed over a time range with a color index.
- **Reset alert thresholds content tile:** You can include call-to-action content tiles and embed a link to an action page. In this case, the reset alert threshold takes you to the application **Jobs**, where you can run updates to device properties. You explore this option later in the [Configure jobs](#) section of this tutorial.
- **Property tiles:** The dashboard displays **Valve operational info**, **Flow alert thresholds**, and **Maintenance info** tiles.

Customize the dashboard

To customize views in the dashboard for operators, select **Edit** on the **Wide World water consumption dashboard**. You can customize the dashboard by selecting the **Edit** menu. After the dashboard is in **edit** mode, you can add new tiles or you can configure it.

To learn more, see [Create and customize dashboards](#).

Explore the device template

In Azure IoT Central, a device template defines the capabilities of a device. Device capabilities include telemetry sent by device sensors, device properties, and commands the device can execute. You can define one or more device templates in Azure IoT Central that represent the capability of the devices that you connect.

The water consumption monitoring application comes with two sample device templates that represent a *flow meter* and a *smart valve* device.

To view the device template:

1. Select **Device templates** on the left pane of your application in Azure IoT Central. In the **Device templates** list, you see two device templates, **Smart Valve** and **Flow meter**.

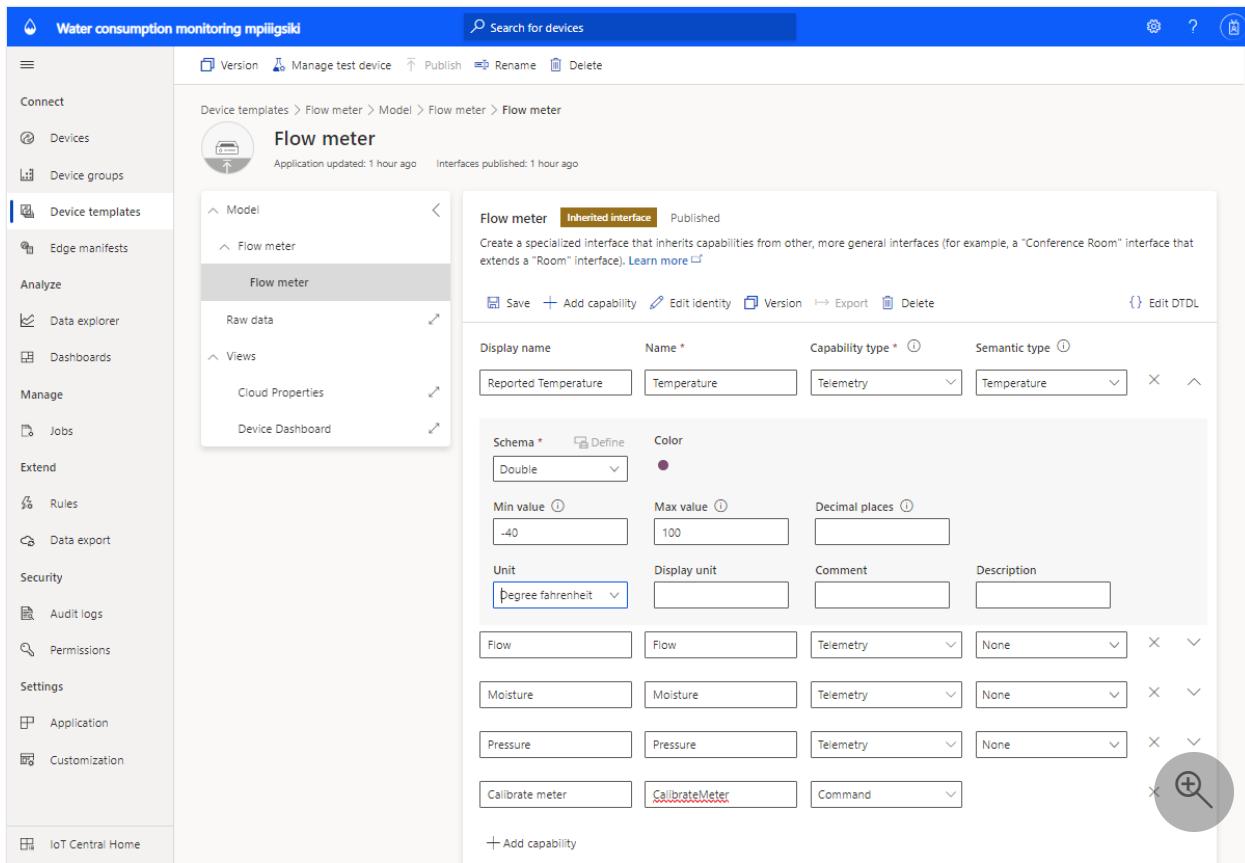
2. Select the **Flow meter** device template, and familiarize yourself with the device capabilities.

Display name	Name	Capability type	Semantic type
Installation location	InstallationLocation	Cloud property	Location
Installation date	InstallationDate	Cloud property	None
Manufacturer	Manufacturer	Cloud property	None
Humidity threshold	HumidityThreshold	Cloud property	None
Max flow threshold	MaxFlowThreshold	Cloud property	None
Serial number	SerialNumber	Cloud property	None
Maintenance contract	MaintenanceContract	Cloud property	None
Flow meter number	FlowMeterNumber	Cloud property	None
Reverse flow threshold	ReverseFlowThreshold	Cloud property	None

Customize the device template

To customize the device template:

1. Navigate to the **Flow Meter** device template.
2. Find the **Temperature** telemetry type.
3. Update the **Display Name** of **Temperature** to **Reported temperature**.
4. Update the unit of measurement, or set the **Min value** and **Max value**.
5. Select **Save** to save any changes.



Add a cloud property

1. Navigate to the **Flow Meter** device template, and select **+ Add capability**.
2. Add a new cloud property by selecting **Cloud Property** as **Capability type**. In Azure IoT Central, you can add a property that is relevant to a device but that doesn't come from the device. For example, a cloud property could be an alerting threshold specific to an installation area, asset information, or other maintenance information.
3. Select **Save** to save any changes.

To learn more, see [Cloud properties](#).

Views

The water consumption monitor device template comes with predefined views. The views define how operators see the device data and set the values of cloud properties.

To learn more, see [Views](#).

Publish the device template

Navigate to device templates page and select **Publish** to save any changes made to the device template.

To learn more, see [How to publish templates](#).

Create a new device template

Select **+** **New** to create a new device template and follow the creation process. You can create a custom device template from scratch or you can choose a device template from the Azure Device Catalog.

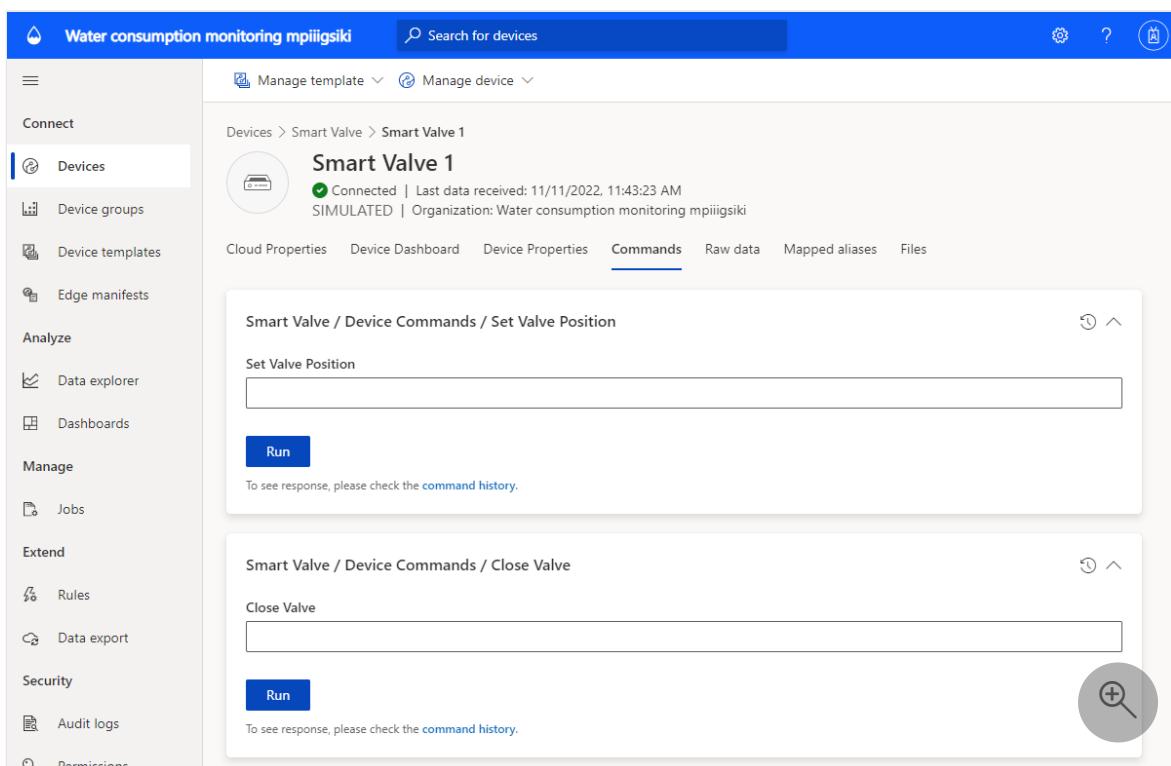
To learn more, see [How to add device templates](#).

Explore simulated devices

In Azure IoT Central, you can create simulated devices to test your device template and application. The water consumption monitoring application has two simulated devices mapped to the **Flow meter** and **Smart Valve** device templates.

View the devices

1. Select **Devices** > **All devices** on the left pane.
2. Select **Smart Valve 1**.
3. On the **Commands** tab, you can see the three device commands (**Close valve**, **Open valve**, and **Set valve position**) that are defined in the **Smart Valve** device template.



The screenshot shows the Azure IoT Central interface for the 'Smart Valve 1' device. The left sidebar is collapsed, and the main content area shows the device details. The 'Commands' tab is selected, displaying three command cards:

- Smart Valve / Device Commands / Set Valve Position**: A text input field labeled 'Set Valve Position' with a 'Run' button below it. A note says 'To see response, please check the command history.'
- Smart Valve / Device Commands / Close Valve**: A text input field labeled 'Close Valve' with a 'Run' button below it. A note says 'To see response, please check the command history.'
- Smart Valve / Device Commands / Open Valve**: A text input field labeled 'Open Valve' with a 'Run' button below it. A note says 'To see response, please check the command history.'

At the bottom right of the main content area is a circular button with a plus sign and a magnifying glass icon.

4. Explore the **Device Properties** tab and the **Device Dashboard** tab.

Note

The views you see on this page are configured using the **Device Template > Views** page.

Add new devices

Add new devices by selecting **+ New** on the **Devices** tab.

To learn more, see [Manage devices](#).

Explore rules

In Azure IoT Central, you can create rules to automatically monitor device telemetry and trigger actions when one or more conditions are met. The actions might include sending email notifications or triggering a Microsoft Power Automate action or a webhook action to send data to other services.

The water consumption monitoring application you created has three preconfigured rules.

View rules

1. Select **Rules** on the left pane.
2. Select **High water flow alert**, which is one of the preconfigured rules in the application.

The screenshot shows the Azure IoT Central interface with the 'Rules' section selected in the left sidebar. The main area displays a 'High water flow alert' rule. The rule is currently disabled. The 'Target devices' section specifies a 'Device template' of 'Flow meter'. The 'Conditions' section defines the rule to trigger if 'all of the conditions are true'. It includes a 'Time aggregation' setting of '60 minutes' and a single condition for 'Flow' where the operator is 'Is greater than' and the aggregation is 'Average'. A 'Value' field is set to 'Max flow threshold'. A search icon is visible in the bottom right of the conditions section.

The **High water flow alert** rule is configured to check against the condition **Flow is greater than** the **Max flow threshold**. Flow threshold is a cloud property defined in the **Smart Valve** device template. The value of **Max flow threshold** is set per device instance.

Next, you can create an email action.

To add an action to the rule:

1. Select **+** **Email**.
2. Enter **High flow alert** as the friendly **Display name** for the action.
3. Enter the email address associated with your Azure IoT Central account in **To**.
4. Optionally, enter a note to include in the text of the email.
5. Select **Done** to complete the action.
6. Select **Save** to save the new rule.
7. Enable the rule.

Within a few minutes, you'll receive an email after the configured condition is met.

ⓘ Note

The application sends an email each time a condition is met. Select **Disable** to disable the rule to stop receiving email from the automated rule.

To create a new rule:

To create a new rule, select **+ New** on the **Rules** tab on the left pane.

Configure jobs

In Azure IoT Central, jobs allow you to trigger device or cloud property updates on multiple devices. In addition to properties, you can also use jobs to trigger device commands on multiple devices. Azure IoT Central automates the workflow for you.

1. Select **Jobs** on the left pane.
2. Select **+ New**, and configure one or more jobs.

To learn more, see [How to run a job](#).

Customize your application

As an administrator, you can change settings to customize the user experience in your application.

Select **Customization > Appearance**, and then:

- To set the masthead logo image, select **Change**.
- To set the browser icon image that appears on browser tabs, select **Change**.
- Under **Browser colors**, you can replace the default browser colors by adding HTML hexadecimal color codes. For more information about color notation for HEX values, see the W3Schools [HTML Colors](#) tutorial.

You can change the application image on the **Application > Management** page.

Clean up resources

If you don't plan to continue using this application, you can delete it:

1. In your Azure IoT Central application, go to **Application > Management**.
2. Select **Delete**, and then confirm your action.

Next steps

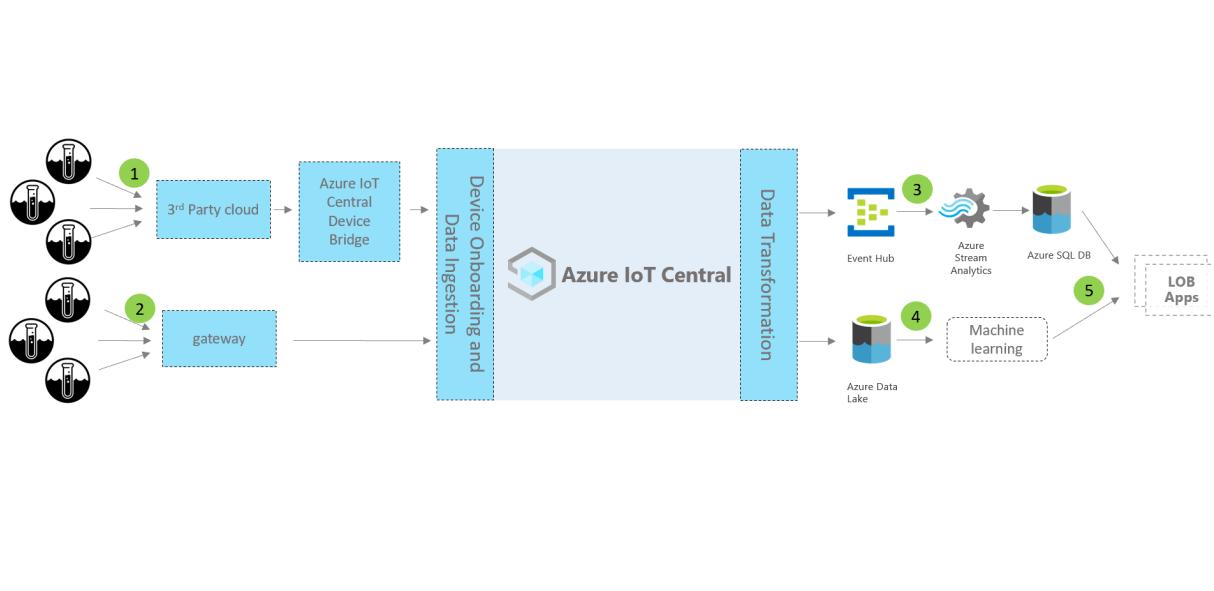
The suggested next step is to learn about [Water quality monitoring](#).

Tutorial: Deploy and walk through the water quality monitoring application

Article • 07/17/2023

Traditional water quality monitoring relies on manual sampling techniques and field laboratory analysis, which is time consuming and costly. Remote water quality monitoring lets you manage water quality issues before citizens are affected. With advanced analytics, water utilities and environmental agencies can act on early warnings of potential water quality issues and plan for water treatment in advance.

The *water quality monitoring* application template helps you kickstart your IoT solution development and enables water utilities to digitally monitor water quality in smart cities.



Devices and connectivity (1,2)

Water management solutions use smart water devices such as flow meters, water quality monitors, smart valves, leak detectors.

Devices in smart water solutions may connect through low-power wide area networks (LPWAN) or through a third-party network operator. For these types of devices, use the [Azure IoT Central Device Bridge](#) to send your device data to your IoT application in Azure IoT Central. You can also use an IP capable device gateway that connects directly to your IoT Central application.

IoT Central

When you build an IoT solution, Azure IoT Central simplifies the build process and helps to reduce the burden and costs of IoT management, operations, and development. You can brand, customize, and integrate your solution with third-party services.

When you connect your smart water devices to IoT Central, the application provides:

- Device command and control.
- Monitoring and alerting.
- A user interface with built-in role-based access controls.
- Configurable dashboards.
- Extensibility options.

Extensibility and integrations (3,4)

You can extend your IoT application in IoT Central and optionally:

- Transform and integrate your IoT data for advanced analytics through data export from your IoT Central application.
- Automate workflows in other systems by triggering actions using Power Automate or webhooks from IoT Central application.
- Programmatically access your IoT Central application by using the IoT Central REST APIs.

Business applications (5)

You can use IoT data to power various business applications within a water utility. In your [IoT Central water consumption monitoring application](#) you can configure rules and actions, and set them to create alerts in [Connected Field Service](#). Configure Power Automate in IoT Central rules to automate workflows across applications and services. Additionally, based on service activities in Connected Field Service, information can be sent back to Azure IoT Central.

In this tutorial, you learn to:

- ✓ Use the **Water quality monitoring** template to create a water quality monitoring application.
- ✓ Explore and customize an dashboard.
- ✓ Explore a water quality monitoring device template.
- ✓ Explore simulated devices.
- ✓ Explore and configure rules.
- ✓ Configure jobs.
- ✓ Customize application branding by using white labeling.

Prerequisites

An active Azure subscription. If you don't have an Azure subscription, create a [free account](#) before you begin.

Create water quality monitoring application

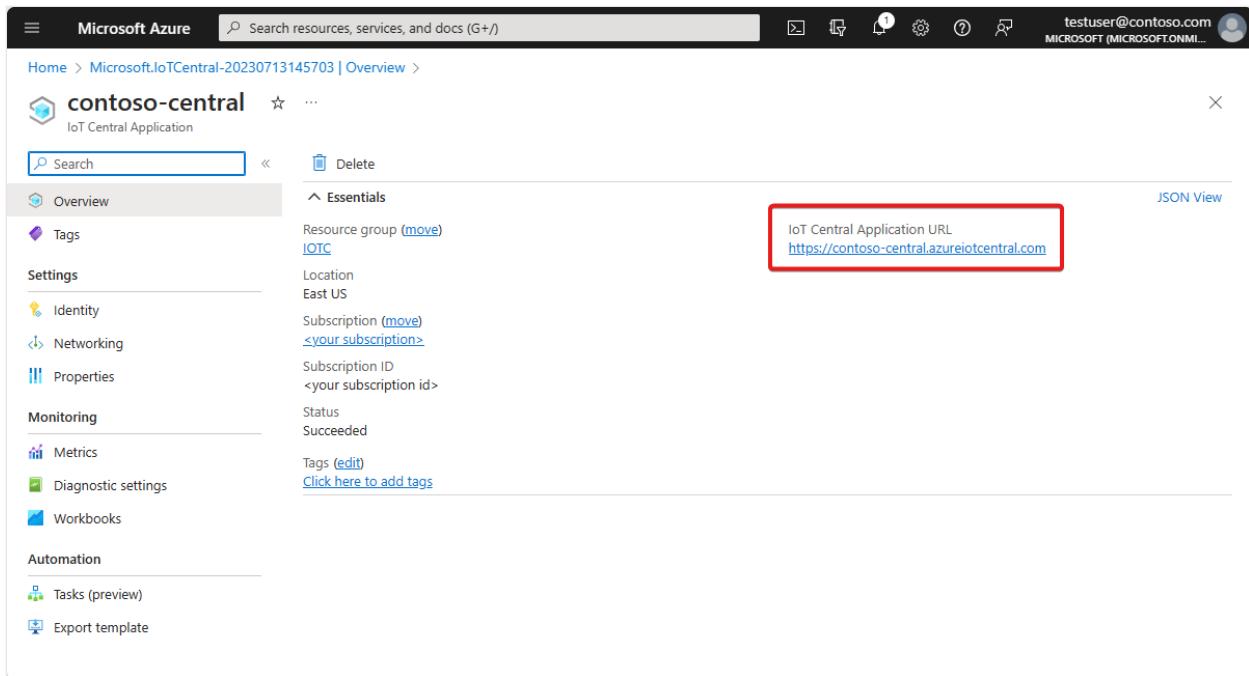
To create your IoT Central application:

1. Navigate to the [Create IoT Central Application](#) page in the Azure portal. If prompted, sign in with your Azure account.
2. Enter the following information:

Field	Description
Subscription	The Azure subscription you want to use.
Resource group	The resource group you want to use. You can create a new resource group or use an existing one.
Resource name	A valid Azure resource name.
Application URL	The URL subdomain for your application. The URL for an IoT Central application looks like <code>https://yoursubdomain.azureiotcentral.com</code> .
Template	Water Consumption Monitoring
Region	The Azure region you want to use.
Pricing plan	The pricing plan you want to use.

3. Select **Review + create**. Then select **Create**.

When the app is ready, you can navigate to it from the Azure portal:



Microsoft Azure Search resources, services, and docs (G+/) testuser@contoso.com MICROSOFT (MICROSOFTONMIL)

Home > Microsoft.IoTCentral-20230713145703 | Overview >

contoso-central IoT Central Application

Search Delete JSON View

Overview ...

Tags

Settings

- Identity
- Networking
- Properties

Monitoring

- Metrics
- Diagnostic settings
- Workbooks

Automation

- Tasks (preview)
- Export template

Essentials

Resource group (move) IOTC

Location East US

Subscription (move) <your subscription>

Subscription ID <your subscription id>

Status Succeeded

Tags (edit) [Click here to add tags](#)

IoT Central Application URL
<https://contoso-central.azureiotcentral.com>

💡 Tip

To list all the IoT Central applications you have access to, navigate to [IoT Central Applications](#).

To learn more, see [Create an Azure IoT Central application](#).

Walk through the application

The following sections walk you through the key features of the application:

Dashboard

After you create the application, the **Wide World water quality** dashboard pane opens.

The screenshot shows the Azure IoT Central interface for a 'Wide World water quality dashboard'. The left sidebar contains navigation links for Connect, Analyze, and Manage, with 'Dashboards' selected. The main area features a logo tile for 'WIDE WORLD WATER UTILITY', three KPI tiles for 'pH' (value -53.76, average past 30 minutes), 'Turbidity (NTU)' (value 38.42, average past 30 minutes), and 'Conductiv' (value 35, average past 30 minutes). Below these are three data visualizations: a 'Water monitoring area map' showing a network of blue lines on a map, a 'pH distribution' heatmap showing a gradient from dark purple to yellow with values -52.08986 and -57.08916, and a 'Critical quality indicators' line chart showing a single data series over time from 11:45 AM to 12:15 PM on 11/11/2022.

As a builder, you can create and customize views on the dashboard for use by operators. Explore the provided dashboard before you start on any customization.

All data shown in the dashboard is based on simulated device data, which is discussed in the next section.

The dashboard includes the following types of tiles:

- **Wide World water utility image tile:** The first tile in the upper-left corner of the dashboard is an image that shows the fictitious utility named Wide World. You can customize the tile to use your own image, or you can remove the tile.
- **Average pH KPI tiles:** KPI tiles like **Average pH in the last 30 minutes** are at the top of the dashboard pane. You can customize KPI tiles and set each to a different type and time range.
- **Water monitoring area map:** Azure IoT Central uses Azure Maps, which you can directly set in your application to show device location. You can also map location information from your application to your device and then use Azure Maps to show the information on a map. Hover over the map and try the controls.
- **Average pH distribution heat-map chart:** You can select different visualizations to show device telemetry in the way that is most appropriate for your application.
- **Critical quality indicators line chart:** You can visualize device telemetry plotted as a line chart over a time range.

- **Concentration of chemical agents bar chart:** You can visualize device telemetry in a bar chart.
- **Reset sensors parameters tile:** The dashboard includes a tile for actions that an operator can initiate directly from the monitoring dashboard such as resetting a device's properties.
- **Property list tiles:** The dashboard has multiple property tiles that represent threshold information, device health information, and maintenance information.

Customize the dashboard

As a builder, you can customize the dashboards for use by operators:

1. Select **Edit** to customize the **Wide World water quality dashboard** pane. You can customize the dashboard by selecting commands on the **Edit** menu. After the dashboard is in edit mode, you can add new tiles, or you can configure the existing files.
2. Select **+ New** to create a new dashboard that you can configure. You can have multiple dashboards and can navigate among them from the dashboard menu.

Explore a water quality monitoring device template

A device template in Azure IoT Central defines the capabilities of a device. Available capabilities are telemetry, properties, and commands. As a builder, you can define device templates in Azure IoT Central that represent the capabilities of the connected devices. You can also create simulated devices to test your device template and application.

The water quality monitoring application you created comes with a water quality monitoring device template.

To view the device template:

1. Select **Device templates** on the leftmost pane of your application in Azure IoT Central.
2. From the list of device templates, select **Water Quality Monitor** to open that device template.

Customize the device template

Practice customizing the following device template settings:

1. Navigate to the **Water Quality Monitor** device template.
2. Go to the **Temperature** telemetry type.
3. Change the **Display name** value to **Reported temperature**.
4. Change the unit of measurement, or set **Min value** and **Max value**.
5. Select **Save**.

Add a cloud property

1. Navigate to the **Water Quality Monitor** device template, and select **+ Add capability**.
2. In Azure IoT Central, you can add a property that is relevant to a device but that doesn't come from the device. One example of such a property is an alert threshold specific to installation area, asset information, or maintenance information.
3. Enter **Installation area** as the **Display name**, select **Cloud property** as the **Capability type** and choose **String** as the **Schema**.
4. Select **Save**.

Explore views

The water quality monitoring device template comes with predefined views. The views define how operators see the device data and set cloud properties. Explore the views

and practice making changes.

Publish the device template

If you make any changes, be sure to select **Publish** to publish the device template.

Create a new device template

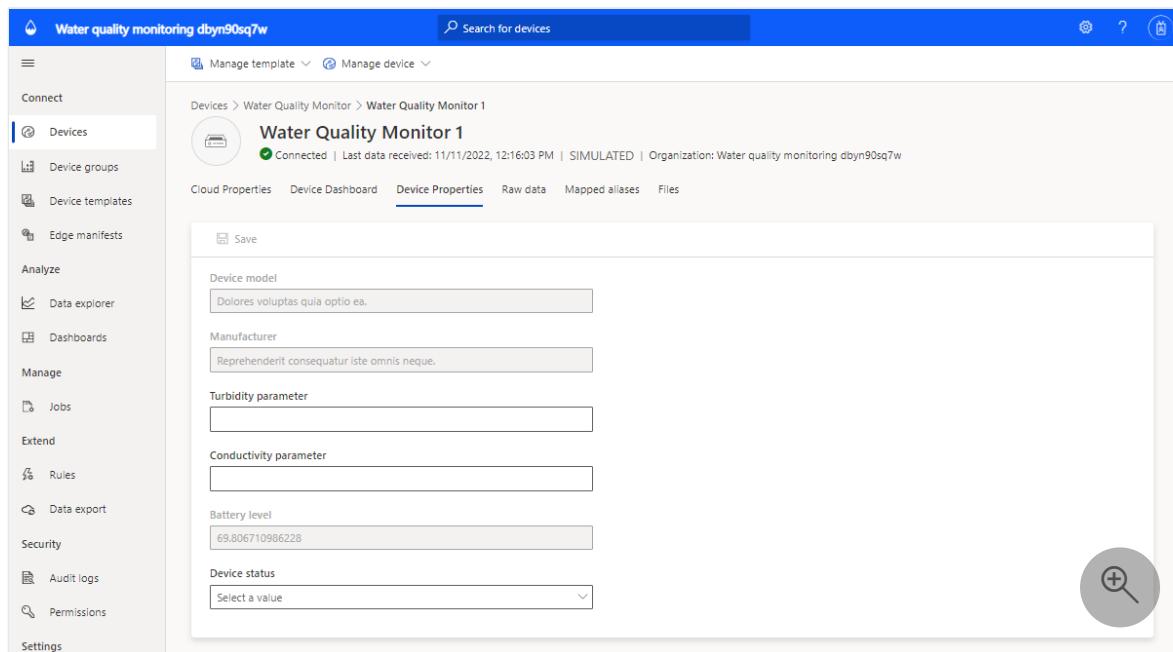
1. On the **Device templates** page, select **+ New** to create a new device template and follow the creation process.
2. Create a custom device template or choose a device template from the Azure IoT device catalog.

Explore simulated devices

The water quality monitoring application you created from the application template has two simulated devices. These devices map to the water quality monitoring device template.

View the devices

1. Select **Devices** on the leftmost pane of your application.
2. Select a simulated device.



The screenshot shows the Azure IoT Device Properties page for a simulated device named 'Water Quality Monitor 1'. The page is titled 'Water quality monitoring dbyn90sq7w'. The left sidebar includes 'Connect', 'Devices' (selected), 'Device groups', 'Device templates', 'Edge manifests', 'Analyze', 'Data explorer', 'Dashboards', 'Manage', 'Jobs', 'Extend', 'Rules', 'Data export', 'Security', 'Audit logs', 'Permissions', and 'Settings'. The top navigation bar has 'Manage template' and 'Manage device' dropdowns, a search bar, and a help icon. The main content area shows the device's status as 'Connected' with the last data received at 11/11/2022, 12:16:03 PM. It is labeled as 'SIMULATED' and part of the organization 'Water quality monitoring dbyn90sq7w'. Below this, tabs for 'Cloud Properties', 'Device Dashboard', 'Device Properties' (selected), 'Raw data', 'Mapped aliases', and 'Files' are visible. The 'Device Properties' tab contains fields for 'Device model' (Dolores voluptas quia optio ea.), 'Manufacturer' (Reprehenderit consequatur iste omnis neque.), 'Turbidity parameter' (empty), 'Conductivity parameter' (empty), 'Battery level' (69.806710986228), and 'Device status' (a dropdown menu with 'Select a value'). A 'Save' button is located at the top of this section. A magnifying glass icon is in the bottom right corner of the main content area.

3. On the **Cloud Properties** tab, change the **Acidity (pH) threshold** value to **9** and select **Save**.

4. Explore the **Device Properties** tab and the **Device Dashboard** tab.

 **Note**

All tabs have been configured from **Device template views**.

Add new devices

1. On the **Devices** tab, select **+ New** to add a new device.
2. Use the suggested **Device ID** or enter your own. You can also enter a **Device name** for your new device.
3. Select **Water Quality Monitor** as the **Device template**.
4. Make sure the **Simulate this device** is set to **Yes** if you want to create a simulated device.
5. Select **Create**.

Explore and configure rules

In Azure IoT Central, you can create rules that automatically monitor device telemetry. These rules trigger an action when any of their conditions are met. One possible action is to send email notifications. Other possibilities include a Power Automate action or a webhook action to send data to other services.

The water quality monitoring application you created has two preconfigured rules.

View rules

1. Select **Rules** on the leftmost pane of your application.
2. Select **High pH alert**, which is one of the preconfigured rules in the application.

The High pH alert rule is configured to check the condition of acidity (pH) being greater than 8.

Next, add an email action to the rule:

1. Select **+** **Email**.
2. In the **Display name** box, enter **High pH alert**.
3. In the **To** box, enter the email address associated with your Azure IoT Central account.
4. Optionally, enter a note to include in the text of the email.
5. Select **Done** to complete the action.
6. Set the rule to **Enabled** and select **Save**.

Within a few minutes, you should receive email when the configured condition is met.

ⓘ Note

The application sends email each time a condition is met. Select **Disable** for a rule to stop receiving automated email from that rule.

To create a new rule, select **Rules** on the leftmost pane of your application and then select **+ New**.

Configure jobs

With Azure IoT Central jobs, you can trigger updates to device or cloud properties on multiple devices. You can also use jobs to trigger device commands on multiple devices. Azure IoT Central automates the workflow for you.

1. Select **Jobs** on the leftmost pane of your application.
2. Select **+New job** and configure one or more jobs.

Customize your application

As an administrator, you can change settings to customize the user experience in your application.

Select **Customization > Appearance**, and then:

- To set the masthead logo image, select **Change**.
- To set the browser icon image that appears on browser tabs, select **Change**.
- Under **Browser colors**, you can replace the default browser colors by adding HTML hexadecimal color codes. For more information about color notation for HEX values, see the W3Schools [HTML Colors](#)  tutorial.

You can change the application image on the **Application > Management** page.

Clean up resources

If you don't plan to continue using this application, you can delete it:

1. In your Azure IoT Central application, go to **Application > Management**.
2. Select **Delete**, and then confirm your action.

Azure Government developer guide

Article • 04/29/2022

Azure Government is a separate instance of the Microsoft Azure service. It addresses the security and compliance needs of United States federal agencies, state and local governments, and their solution providers. Azure Government enforces physical isolation from non-US government infrastructure and relies on [screened US personnel](#) for operations.

Microsoft provides various tools to help you create and deploy cloud applications on global Azure and Azure Government.

When you create and deploy applications on Azure Government, you need to know the key differences between Azure Government and global Azure. The specific areas to understand are:

- Setting up and configuring your programming environment
- Configuring endpoints
- Writing applications
- Deploying applications as services to Azure Government

The information in this document summarizes the differences between the two cloud environments. It supplements the information that's available through the following sources:

- [Azure Government](#) ↗ site
- [Microsoft Trust Center](#) ↗
- [Azure documentation center](#)
- [Azure Blogs](#) ↗

This content is intended for Microsoft partners and developers who are deploying to Azure Government.

Guidance for developers

Most of the currently available technical content assumes that applications are being developed on global Azure rather than on Azure Government. For this reason, it's important to be aware of two key differences in applications that you develop for hosting in Azure Government.

- Certain services and features that are in specific regions of global Azure might not be available in Azure Government.

- Feature configurations in Azure Government might differ from those in global Azure.

Therefore, it's important to review your sample code and configurations to ensure that you are building within the Azure Government cloud services environment.

Endpoint mapping

Service endpoints in Azure Government are different than in Azure. For a mapping between Azure and Azure Government endpoints, see [Compare Azure Government and global Azure](#).

Feature variations

For current Azure Government regions and available services, see [Products available by region](#). Services available in Azure Government are listed by category and whether they are Generally Available or available through Preview. In general, service availability in Azure Government implies that all corresponding service features are available to you. Variations to this approach and other applicable limitations are tracked and explained in [Compare Azure Government and global Azure](#).

Quickstarts

Navigate through the following links to get started using Azure Government:

- [Login to Azure Government portal](#)
- [Connect with PowerShell](#)
- [Connect with CLI](#)
- [Connect with Visual Studio](#)
- [Connect to Azure Storage](#)
- [Connect with Azure SDK for Python](#)

Azure Government Video Library

The [Azure Government video library](#) contains many helpful videos to get you up and running with Azure Government.

Compliance

For more information about Azure Government compliance assurances, see [Azure Government compliance](#) documentation.

Next steps

For more information about Azure Government, see the following resources:

- [Sign up for a trial ↗](#)
- [Acquiring and accessing Azure Government ↗](#)
- [Ask questions via the azure-gov tag in StackOverflow ↗](#)
- [Azure Government blog ↗](#)
- [Azure Government overview](#)
- [Azure Government security](#)
- [Compare Azure Government and global Azure](#)
- [Azure Government compliance](#)
- [Azure compliance](#)

Develop with Storage API on Azure Government

Article • 10/26/2022

Azure Government uses the same underlying technologies as commercial Azure, enabling you to use the development tools you're already familiar with. If you don't have an Azure Government subscription, create a [free account](#) before you begin.

Prerequisites

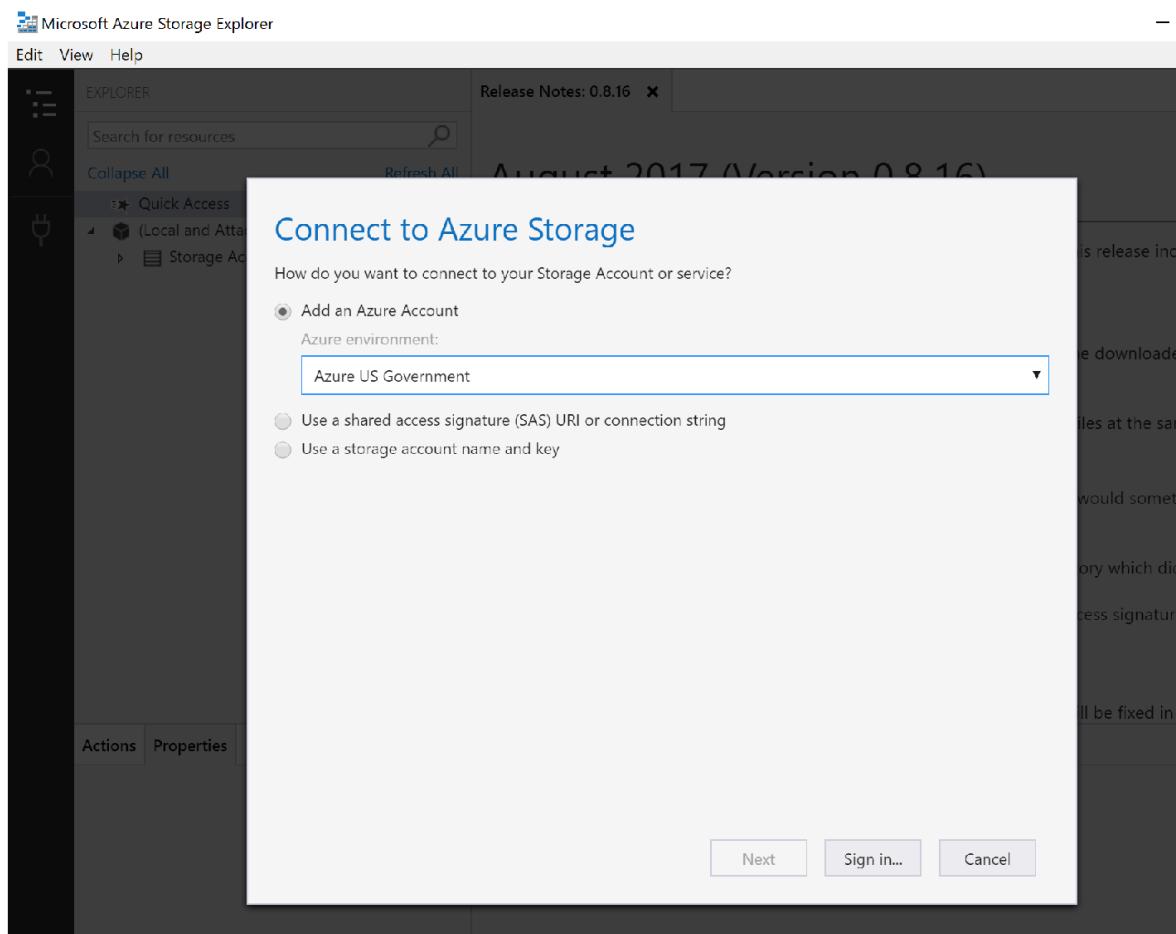
- Review [Guidance for developers](#). This article discusses Azure Government's unique URLs and endpoints for managing your environment. You must know about these endpoints to connect to Azure Government.
- Review [Compare Azure Government and global Azure](#) and click on a service of interest to see variations between Azure Government and global Azure.
- Download and install the latest version of [Azure Storage Explorer](#).

Connecting Storage Explorer to Azure Government

The [Microsoft Azure Storage Explorer](#) is a cross-platform tool for working with Azure Storage. Government customers can now take advantage of all the latest features of the Azure Storage Explorer such as creating and managing blobs, queues, tables, and file shares.

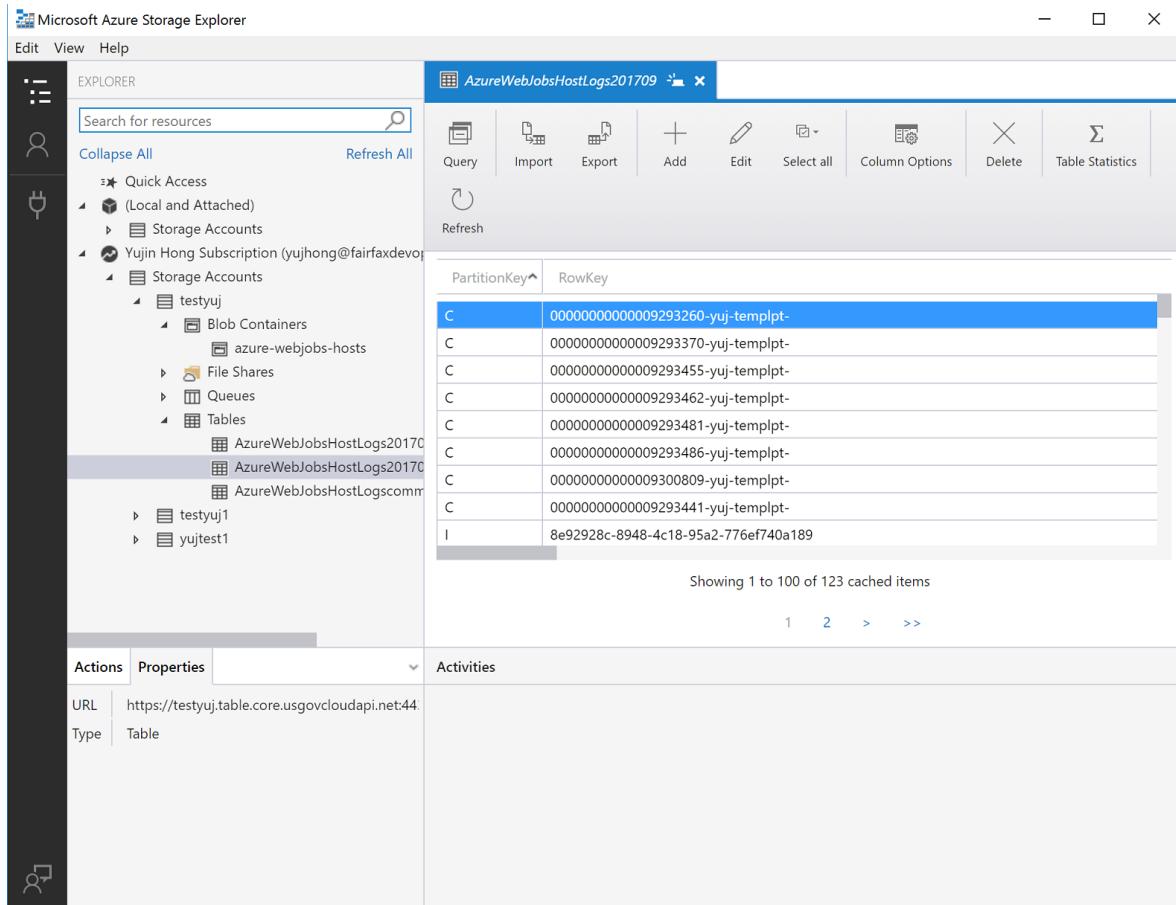
Getting Started with Storage Explorer

1. Open the Azure Storage Explorer desktop application.
2. You'll be prompted to add an Azure account; in the dropdown choose the "Azure US Government" option:



3. Sign in to your Azure Government account and you can see all of your resources.

The Storage Explorer should look similar to the screenshot below. Click on your Storage Account to see the blob containers, file shares, Queues, and Tables.



For more information about Azure Storage Explorer, see [Get started with Storage Explorer](#).

Connecting to the Storage API

Prerequisites

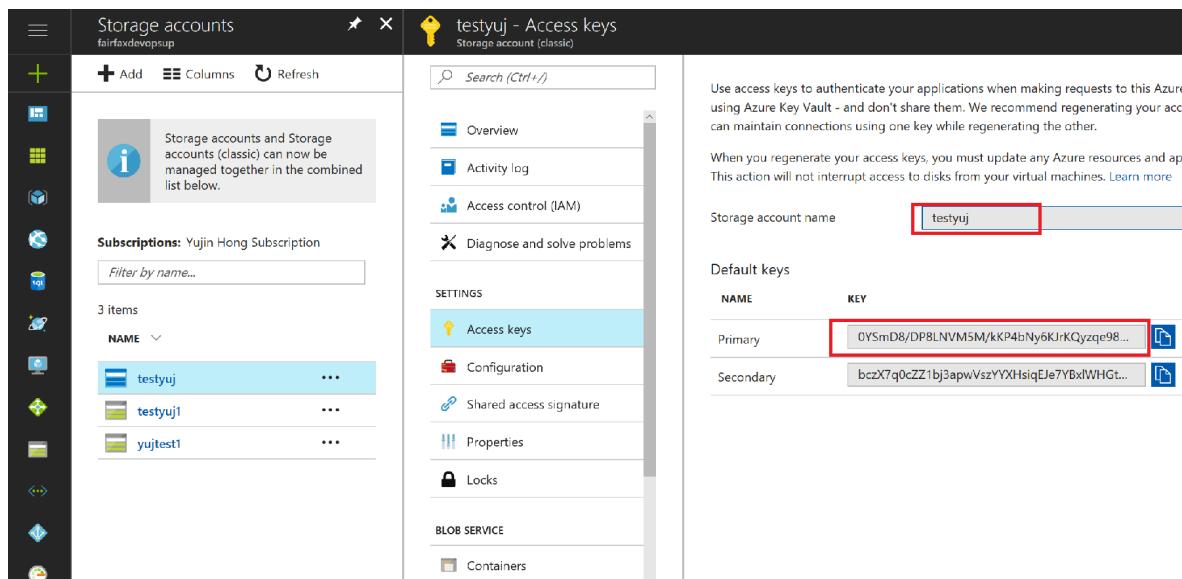
- Have an active Azure Government subscription. If you don't have an Azure Government subscription, create a [free account](#) before you begin.
- Download Visual Studio 2019.

Getting Started with Storage API

One important difference to remember when connecting with the Storage API is that the URL for storage in Azure Government is different than the URL for storage in commercial Azure. Specifically, the domain ends with "core.usgovcloudapi.net", rather than "core.windows.net".

These endpoint differences must be taken into account when you connect to storage in Azure Government with C#.

1. Go to the [Azure Government portal](#) and select your storage account and then click the "Access Keys" tab:



The screenshot shows the Azure Government portal interface. On the left, there is a sidebar with various icons. The main area is titled "Storage accounts" and shows a list of storage accounts under "Subscriptions: Yujin Hong Subscription". The account "testyuj" is selected and highlighted in blue. To the right, a detailed view for "testyuj" is shown under the "Access keys" tab. The "Access keys" section is highlighted with a red box. It shows two keys: "Primary" with the key value "0YSmD8/DPBLNVMSM/kKP4bNy6KjRKQyzqe98...". The "Secondary" key value is partially visible as "bczX7q0cZZ1bj3apwVs...". Below the keys, there are sections for "Configuration", "Shared access signature", "Properties", and "Locks". At the bottom, there are "BLOB SERVICE" and "Containers" sections.

2. Copy/paste the storage account connection string.

C#

1. Open Visual Studio and create a new project. Add a reference to the [Azure Tables client library for .NET](#). This package contains classes for connecting to your Storage Table account.
2. Add these two lines of C# code to connect:

```
C#
```

```
var credentials = new TableSharedKeyCredential(storageAccountName,
Environment.GetEnvironmentVariable("STORAGE_ACCOUNT_KEY"));
var storageTableUri =
Environment.GetEnvironmentVariable("STORAGE_TABLE_URI");
var tableServiceClient = new TableServiceClient(new
Uri(storageTableUri), credentials);
```

3. At this point, we can interact with Storage as we normally would. For example, if we want to retrieve a specific entity from our Table Storage, we could do it like this:

```
C#
```

```
var tableClient = tableServiceClient.GetTableClient("Contacts");
ContactEntity contact = tableClient.GetEntity<ContactEntity>("gov-
partition1", "0fb52a6c-3784-4dc5-aa6d-ecda4426dbda");
Console.WriteLine($"Contact: {contact.FirstName} {contact.LastName}");
```

Java

1. Download the [Azure Tables client library for Java](#) and configure your project correctly.
2. Create a "test" class where we'll access Azure Table Storage using the Azure Tables client library.
Copy and paste the code below, and **paste** your Storage Account connection string into the `AZURE_STORAGE_CONNECTION_STRING` environment variable.

```
Java
```

```
import com.azure.data.tables.implementation.ModelHelper;
import com.azure.data.tables.models.*;
import java.util.HashMap;
public class test {
    public static final String storageConnectionString =
System.getenv("AZURE_STORAGE_CONNECTION_STRING");
    public static void main(String[] args) {
        try
        {
            // Create the table service client.
```

```
    TableServiceClient tableServiceClient = new
TableServiceClientBuilder()
    .connectionString(storageConnectionString)
    .buildClient();
    // Create the table if it doesn't exist.
    String tableName = "Contacts";
    TableClient tableClient =
tableServiceClient.createTableIfNotExists(tableName);
    // Create a new customer entity.
    TableEntity customer1 = ModelHelper.createEntity(new
HashMap<String, Object>() {{
        put("PartitionKey", "Brown");
        put("RowKey", "Walter");
        put("Email", "Walter@contoso.com");
    }});
    // Insert table entry into table
    tableClient.createEntity(customer1);
}
catch (Exception e)
{
    // Output the stack trace.
    e.printStackTrace();
}
}
```

Node.js

1. Download the [Azure Storage Blob client library for Node.js](#) and configure your application correctly.
 2. The following code below connects to Azure Blob Storage and creates a Container using the Azure Storage API. **Paste** your Azure Storage account connection string into the `AZURE STORAGE CONNECTION STRING` environment variable.

JavaScript

```
var { BlobServiceClient } = require("@azure/storage-blob");
var storageConnectionString =
process.env[ "AZURE_STORAGE_CONNECTION_STRING" ];
var blobServiceClient =
BlobServiceClient.fromConnectionString(storageConnectionString);
var containerClient = blobServiceClient.getContainerClient('testing');
containerClient.createIfNotExists();
```

Python

1. Download the [Azure Storage Blob client library for Python](#).

2. When using the Storage library for Python to connect to Azure Government, paste your Azure storage connection string in the `AZURE_STORAGE_CONNECTION_STRING` environment variable.

Python

```
# Create the BlobServiceClient that is used to call the Blob service
# for the storage account
connection_string = os.getenv("AZURE_STORAGE_CONNECTION_STRING")
blob_service_client =
    BlobServiceClient.from_connection_string(conn_str=connection_string)
container_name = 'ml-gov-demo'
container =
    blob_service_client.get_container_client(container=container_name)
generator = container.list_blobs()
for blob in generator:
    print("\t Blob name: " + blob.name)
```

PHP

1. Download the [Azure Storage SDK for PHP](#).
2. The code below accesses Azure Table Storage using the Azure Storage API. In the `connectionString` variable, you'll notice that there's a `TableEndpoint` parameter. Depending on which service you're using, you must define the parameter and set it to the endpoint for that service:
 - `BlobEndpoint`= //ends with 'blob.core.usgovcloudapi.net'
 - `QueueEndpoint`= //ends with 'queue.core.usgovcloudapi.net'
 - `TableEndpoint`= //ends with 'table.core.usgovcloudapi.net'

 **Note**

You can find these endpoints by navigating to your Storage Account from the [portal](#). Paste in your storage account name, key, and service endpoint in the `connectionString` variable.

PHP

```
<?php
require_once "vendor/autoload.php";
use WindowsAzure\Common\ServicesBuilder;
use MicrosoftAzure\Storage\Common\ServiceException;
```

```
$connectionString = 'DefaultEndpointsProtocol=http;AccountName=
<accountname>;AccountKey=
<accountkey>;TableEndpoint=http://<storageaccountname>.table.core.
usgovcloudapi.net/';

$tableRestProxy = ServicesBuilder::getInstance()->createTableService($connectionString);
try {
// Create table.
$tableRestProxy->createTable("test");
}
catch(ServiceException $e){
$code = $e->getCode();
$error_message = $e->getMessage();
}
?>
```

Next steps

- Read more about [Azure Storage](#).
- Subscribe to the [Azure Government blog](#) ↗
- Get help on Stack Overflow by using the [azure-gov](#) ↗ tag

Azure AI services on Azure Government

Article • 07/28/2023

This article provides developer guidance for using Computer Vision, Face API, Text Analytics, and Translator Azure AI services. For feature variations and limitations, see [Compare Azure Government and global Azure](#).

Prerequisites

Note

We recommend that you use the Azure Az PowerShell module to interact with Azure. See [Install Azure PowerShell](#) to get started. To learn how to migrate to the Az PowerShell module, see [Migrate Azure PowerShell from AzureRM to Az](#).

- Install and Configure [Azure PowerShell](#)
- Connect [PowerShell with Azure Government](#)

Part 1: Provision Azure AI services accounts

In order to access any of the Azure AI services APIs, you must first provision an Azure AI services account for each of the APIs you want to access. You can create Azure AI services in the [Azure Government portal](#), or you can use Azure PowerShell to access the APIs and services as described in this article.

Note

You must go through the process of creating an account and retrieving account key (explained below) **for each** of the APIs you want to access.

1. Make sure that you have the [Cognitive Services resource provider registered on your account](#).

You can do this by **running the following PowerShell command**:

PowerShell

```
Get-AzResourceProvider
```

If you do **not** see `Microsoft.CognitiveServices`, you have to register the resource provider by **running the following command**:

PowerShell

```
Register-AzResourceProvider -ProviderNamespace  
Microsoft.CognitiveServices
```

2. In the PowerShell command below, replace `rg-name`, `name-of-your-api`, and `location-of-resourcegroup` with your relevant account information.

Replace the `<type of API>` tag with any of the following APIs you want to access:

- ComputerVision
- Face
- TextAnalytics
- TextTranslation

PowerShell

```
New-AzCognitiveServicesAccount -ResourceGroupName 'rg-name' -name  
'name-of-your-api' -Type <type of API> -SkuName S0 -Location 'location-  
of-resourcegroup'
```

Example:

PowerShell

```
New-AzCognitiveServicesAccount -ResourceGroupName 'resourcegroup1' -  
name 'myFaceAPI' -Type Face -SkuName S0 -Location 'usgovvirginia'
```

After you run the command, you should see something like this:

```
ResourceGroupName : myResourceGroup1  
AccountName     : myComputerVisionAPI  
Id              : XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX  
Endpoint        : https://virginia.api.cognitive.microsoft.us/vision/v1.0  
Location        : usgovvirginia  
Sku              : Microsoft.Azure.Management.CognitiveServices.Models.Sku  
AccountType     : ComputerVision  
ResourceType    : Microsoft.CognitiveServices/accounts  
Etag             : XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX  
Provisioningstate : succeeded  
Tags             : XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX
```

3. Copy and save the "Endpoint" attribute somewhere as you will need it when making calls to the API.

Retrieve Account Key

You must retrieve an account key to access the specific API.

In the PowerShell command below, replace the `<youraccountname>` tag with the name that you gave the Account that you created above. Replace the `rg-name` tag with the name of your resource group.

PowerShell

```
Get-AzCognitiveServicesAccountKey -Name <youraccountname> -ResourceGroupName  
'rg-name'
```

Example:

PowerShell

```
Get-AzCognitiveServicesAccountKey -Name myFaceAPI -ResourceGroupName  
'resourcegroup1'
```

Copy and save the first key somewhere as you will need it to make calls to the API.

Key1

Key2

Now you are ready to make calls to the APIs.

Part 2: API Quickstarts

The Quickstarts below will help you to get started with the APIs available through Azure AI services in Azure Government.

Computer Vision

Prerequisites

- Get the [Microsoft Computer Vision API Windows SDK](#).
- Make sure Visual Studio has been installed:
 - [Visual Studio 2019](#), including the **Azure development** workload.

 Note

After you install or upgrade to Visual Studio 2019, you might also need to manually update the Visual Studio 2019 tools for Azure Functions. You can update the tools from the **Tools** menu under **Extensions and Updates... > Updates > Visual Studio Marketplace > Azure Functions and Web Jobs Tools > Update**.

Variations

- The URI for accessing Computer Vision in Azure Government is different than in Azure. For a list of Azure Government endpoints, see [Compare Azure Government and global Azure](#).

Analyze an image with Computer Vision using C#

With the [Analyze Image method](#), you can extract visual features based on image content. You can upload an image or specify an image URL and choose which features to return, including:

- A detailed list of tags related to the image content.
- A description of image content in a complete sentence.
- The coordinates, gender, and age of any faces contained in the image.
- The ImageType (clip art or a line drawing).
- The dominant color, the accent color, or whether an image is black & white.
- The category defined in this [taxonomy](#).
- Does the image contain adult or sexually suggestive content?

Analyze an image C# example request

1. Create a new Console solution in Visual Studio.
2. Replace Program.cs with the following code.
3. Change the `uriBase` to the "Endpoint" attribute that you saved from Part 1, and keep the "/analyze" after the endpoint.
4. Replace the `subscriptionKey` value with your valid subscription key.
5. Run the program.

C#

```
using System;
using System.IO;
using System.Net.Http;
using System.Net.Http.Headers;
using System.Text;
```

```

namespace VisionApp1
{
    static class Program
    {
        // ****
        // *** Update or verify the following values. ***
        // ****

        // Replace the subscriptionKey string value with your valid
        subscription key.
        const string subscriptionKey = "<subscription key>";

        //Copy and paste the "Endpoint" attribute that you saved before
        into the uriBase string "/analyze" at the end.
        //Example:
        https://virginia.api.cognitive.microsoft.us/vision/v1.0/analyze

        const string uriBase = "<endpoint>/analyze";

        static void Main()
        {
            // Get the path and filename to process from the user.
            Console.WriteLine("Analyze an image:");
            Console.Write("Enter the path to an image you wish to
analyze: ");
            string imagePath = Console.ReadLine();

            // Execute the REST API call.
            MakeAnalysisRequest(imagePath);

            Console.WriteLine("\nPlease wait a moment for the results to
appear. Then, press Enter to exit...\n");
            Console.ReadLine();
        }

        /// <summary>
        /// Gets the analysis of the specified image file by using the
        Computer Vision REST API.
        /// </summary>
        /// <param name="imageFilePath">The image file.</param>
        static async void MakeAnalysisRequest(string imagePath)
        {
            HttpClient client = new HttpClient();

            // Request headers.
            client.DefaultRequestHeaders.Add("Ocp-Apim-Subscription-
Key", subscriptionKey);

            // Request parameters. A third optional parameter is
            "details".
            string requestParameters =
            "visualFeatures=Categories,Description,Color&language=en";
        }
    }
}

```

```

        // Assemble the URI for the REST API Call.
        string uri = uriBase + "?" + requestParameters;

        HttpResponseMessage response;

        // Request body. Posts a locally stored JPEG image.
        byte[] byteData = GetImageAsByteArray(imageFilePath);

        using (ByteArrayContent content = new
ByteArrayContent(byteData))
{
    // This example uses content type "application/octet-
stream".
    // The other content types you can use are
    "application/json" and "multipart/form-data".
    content.Headers.ContentType = new
MediaTypeHeaderValue("application/octet-stream");

    // Execute the REST API call.
    response = await client.PostAsync(uri, content);

    // Get the JSON response.
    string contentString = await
response.Content.ReadAsStringAsync();

    // Display the JSON response.
    Console.WriteLine("\nResponse:\n");
    Console.WriteLine(JsonPrettyPrint(contentString));
}
}

/// <summary>
/// Returns the contents of the specified file as a byte array.
/// </summary>
/// <param name="imageFilePath">The image file to read.</param>
/// <returns>The byte array of the image data.</returns>
static byte[] GetImageAsByteArray(string imagePath)
{
    FileStream fileStream = new FileStream(imagePath,
 FileMode.Open, FileAccess.Read);
    BinaryReader binaryReader = new BinaryReader(fileStream);
    return binaryReader.ReadBytes((int)fileStream.Length);
}

/// <summary>
/// Formats the given JSON string by adding line breaks and
indents.
/// </summary>
/// <param name="json">The raw JSON string to format.</param>
/// <returns>The formatted JSON string.</returns>
static string JsonPrettyPrint(string json)
{
    if (string.IsNullOrEmpty(json))

```

```
        return string.Empty;

    json = json.Replace(Environment.NewLine, "").Replace("\t",
"");

    StringBuilder sb = new StringBuilder();
    bool quote = false;
    bool ignore = false;
    int offset = 0;
    int indentLength = 3;

    foreach (char ch in json)
    {
        switch (ch)
        {
            case '':
                if (!ignore) quote = !quote;
                break;
            case '\'':
                if (quote) ignore = !ignore;
                break;
        }

        if (quote)
            sb.Append(ch);
        else
        {
            switch (ch)
            {
                case '{':
                case '[':
                    sb.Append(ch);
                    sb.Append(Environment.NewLine);
                    sb.Append(new string(' ', ++offset *
indentLength));
                    break;
                case '}':
                case ']':
                    sb.Append(Environment.NewLine);
                    sb.Append(new string(' ', --offset *
indentLength));
                    break;
                case ',':
                    sb.Append(ch);
                    sb.Append(Environment.NewLine);
                    sb.Append(new string(' ', offset *
indentLength));
                    break;
                case ':':
                    sb.Append(ch);
                    sb.Append(' ');
                    break;
                default:
                    if (ch != ' ') sb.Append(ch);
            }
        }
    }
}
```

```
        break;
    }
}

return sb.ToString().Trim();
}
}
}
```

Analyze an Image response

A successful response is returned in JSON. Shown below is an example of a successful response:

JSON

```
{
  "categories": [
    {
      "name": "people_baby",
      "score": 0.52734375
    },
    {
      "name": "people_young",
      "score": 0.4375
    }
  ],
  "description": {
    "tags": [
      "person",
      "indoor",
      "clothing",
      "woman",
      "white",
      "table",
      "food",
      "girl",
      "smiling",
      "posing",
      "holding",
      "black",
      "sitting",
      "young",
      "plate",
      "hair",
      "wearing",
      "cake",
      "large",
      "shirt",
      "dress",
      "tablecloth"
    ]
  }
}
```

```
        "eating",
        "standing",
        "blue"
    ],
    "captions": [
        {
            "text": "a woman posing for a picture",
            "confidence": 0.460196158842535
        }
    ]
},
"requestId": "7c20cc50-f5eb-453b-abb5-98378917431c",
"metadata": {
    "width": 721,
    "height": 960,
    "format": "Jpeg"
},
"color": {
    "dominantColorForeground": "Black",
    "dominantColorBackground": "White",
    "dominantColors": [
        "White"
    ],
    "accentColor": "7C4F57",
    "isBWImg": false
}
}
```

For more information, see [public documentation](#) and [public API documentation](#) for Computer Vision.

Face API

Prerequisites

- Get the [Microsoft Face API Windows SDK](#).
- Make sure Visual Studio has been installed:
 - [Visual Studio 2019](#), including the **Azure development** workload.

Note

After you install or upgrade to Visual Studio 2019, you might also need to manually update the Visual Studio 2019 tools for Azure Functions. You can update the tools from the **Tools** menu under **Extensions and Updates...** >

Variations

- The URI for accessing the Face API in Azure Government is different than in Azure. For a list of Azure Government endpoints, see [Compare Azure Government and global Azure](#).

Detect faces in images with Face API using C#

Use the [Face - Detect method](#) to detect faces in an image and return face attributes including:

- Face ID: Unique ID used in several Face API scenarios.
- Face Rectangle: The left, top, width, and height indicating the location of the face in the image.
- Landmarks: An array of 27-point face landmarks pointing to the important positions of face components.
- Facial attributes including age, gender, smile intensity, head pose, and facial hair.

Face detect C# example request

The sample is written in C# using the Face API client library.

1. Create a new Console solution in Visual Studio.
2. Replace Program.cs with the following code.
3. Replace the `subscriptionKey` value with the key value that you retrieved above.
4. Change the `uriBase` value to the "Endpoint" attribute you retrieved above.
5. Run the program.
6. Enter the path to an image on your hard drive.

C#

```
using System;
using System.IO;
using System.Net.Http;
using System.Net.Http.Headers;
using System.Text;

namespace FaceApp1
{
```

```

static class Program
{
    // ****
    // *** Update or verify the following values. ***
    // ****

    // Replace the subscriptionKey string value with your valid
    subscription key.
    const string subscriptionKey = "<subscription key>";

    //Copy and paste the "Endpoint" attribute that you saved before into
    the uriBase string "/detect" at the end.
    //Example:
    https://virginia.api.cognitive.microsoft.us/face/v1.0/detect
    const string uriBase = "<endpoint>/detect";

    static void Main()
    {
        // Get the path and filename to process from the user.
        Console.WriteLine("Detect faces:");
        Console.Write("Enter the path to an image with faces that you
        wish to analyze: ");
        string imagePath = Console.ReadLine();

        // Execute the REST API call.
        MakeAnalysisRequest(imagePath);

        Console.WriteLine("\nPlease wait a moment for the results to
        appear. Then, press Enter to exit...\n");
        Console.ReadLine();
    }

    /// <summary>
    /// Gets the analysis of the specified image file by using the
    Computer Vision REST API.
    /// </summary>
    /// <param name="imageFilePath">The image file.</param>
    static async void MakeAnalysisRequest(string imagePath)
    {
        HttpClient client = new HttpClient();

        // Request headers.
        client.DefaultRequestHeaders.Add("Ocp-Apim-Subscription-Key",
        subscriptionKey);

        // Request parameters. A third optional parameter is "details".
        string requestParameters =
"returnfaceId=true&returnfaceLandmarks=false&returnfaceAttributes=age,gender
,headPose,smile,facialHair,glasses,emotion";

        // Assemble the URI for the REST API Call.
        string uri = uriBase + "?" + requestParameters;
    }
}

```

```

    HttpResponseMessage response;

    // Request body. Posts a locally stored JPEG image.
    byte[] byteData = GetImageAsByteArray(imageFilePath);

    using (ByteArrayContent content = new
ByteArrayContent(byteData))
    {
        // This example uses content type "application/octet-
stream".
        // The other content types you can use are
"application/json" and "multipart/form-data".
        content.Headers.ContentType = new
MediaTypeHeaderValue("application/octet-stream");

        // Execute the REST API call.
        response = await client.PostAsync(uri, content);

        // Get the JSON response.
        string contentString = await
response.Content.ReadAsStringAsync();

        // Display the JSON response.
        Console.WriteLine("\nResponse:\n");
        Console.WriteLine(JsonPrettyPrint(contentString));
    }
}

/// <summary>
/// Returns the contents of the specified file as a byte array.
/// </summary>
/// <param name="imageFilePath">The image file to read.</param>
/// <returns>The byte array of the image data.</returns>
static byte[] GetImageAsByteArray(string imagePath)
{
    FileStream fileStream = new FileStream(imagePath,
 FileMode.Open, FileAccess.Read);
    BinaryReader binaryReader = new BinaryReader(fileStream);
    return binaryReader.ReadBytes((int)fileStream.Length);
}

/// <summary>
/// Formats the given JSON string by adding line breaks and indents.
/// </summary>
/// <param name="json">The raw JSON string to format.</param>
/// <returns>The formatted JSON string.</returns>
static string JsonPrettyPrint(string json)
{
    if (string.IsNullOrEmpty(json))
        return string.Empty;

    json = json.Replace(Environment.NewLine, "").Replace("\t", "");
}

```

```

StringBuilder sb = new StringBuilder();
bool quote = false;
bool ignore = false;
int offset = 0;
int indentLength = 3;

foreach (char ch in json)
{
    switch (ch)
    {
        case '':
            if (!ignore) quote = !quote;
            break;
        case '\'':
            if (quote) ignore = !ignore;
            break;
    }

    if (quote)
        sb.Append(ch);
    else
    {
        switch (ch)
        {
            case '{':
            case '[':
                sb.Append(ch);
                sb.Append(Environment.NewLine);
                sb.Append(new string(' ', ++offset *
indentLength));
                break;
            case '}':
            case ']':
                sb.Append(Environment.NewLine);
                sb.Append(new string(' ', --offset *
indentLength));
                break;
            case ',':
                sb.Append(ch);
                sb.Append(Environment.NewLine);
                sb.Append(new string(' ', offset *
indentLength));
                break;
            case ':':
                sb.Append(ch);
                sb.Append(' ');
                break;
            default:
                if (ch != ' ') sb.Append(ch);
                break;
        }
    }
}

```

```
        return sb.ToString().Trim();
    }
}
}
```

Face detect response

A successful response is returned in JSON. Shown below is an example of a successful response:

JSON

Response:

```
[  
  {  
    "faceId": "0ed7f4db-1207-40d4-be2e-84694e42d682",  
    "faceRectangle": {  
      "top": 60,  
      "left": 83,  
      "width": 361,  
      "height": 361  
    },  
    "faceAttributes": {  
      "smile": 0.284,  
      "headPose": {  
        "pitch": 0.0,  
        "roll": -12.2,  
        "yaw": -16.7  
      },  
      "gender": "female",  
      "age": 16.5,  
      "facialHair": {  
        "moustache": 0.0,  
        "beard": 0.0,  
        "sideburns": 0.0  
      },  
      "glasses": "NoGlasses",  
      "emotion": {  
        "anger": 0.003,  
        "contempt": 0.001,  
        "disgust": 0.001,  
        "fear": 0.002,  
        "happiness": 0.284,  
        "neutral": 0.694,  
        "sadness": 0.012,  
        "surprise": 0.004  
      }  
    }  
  }  
]
```

For more information, see [public documentation](#), and [public API documentation](#) for Face API.

Text Analytics

For instructions on how to use Text Analytics, see [Quickstart: Use the Text Analytics client library and REST API](#).

Variations

- The URI for accessing Text Analytics in Azure Government is different than in Azure. For a list of Azure Government endpoints, see [Compare Azure Government and global Azure](#).

Translator

Prerequisites

- Make sure Visual Studio has been installed:
 - [Visual Studio 2019](#), including the **Azure development** workload.

ⓘ Note

After you install or upgrade to Visual Studio 2019, you might also need to manually update the Visual Studio 2019 tools for Azure Functions. You can update the tools from the **Tools** menu under **Extensions and Updates...** > **Updates** > **Visual Studio Marketplace** > **Azure Functions and Web Jobs Tools** > **Update**.

Variations

- The URI for accessing Translator in Azure Government is different than in Azure. For a list of Azure Government endpoints, see [Compare Azure Government and global Azure](#).
- [Virtual Network support](#) for Translator service is limited to only [US Gov Virginia](#) region. The URI for accessing the API is:
 - `https://<your-custom-domain>.cognitiveservices.azure.us/translator/text/v3.0`

- You can find your custom domain endpoint in the overview blade on the Azure Government portal once the resource is created.
- There are 2 regions: `US Gov Virginia` and `US Gov Arizona`.

Text translation method

The below example uses [Text Translation - Translate method](#) to translate a string of text from a language into another specified language. There are multiple [language codes](#) that can be used with Translator.

Text translation C# example request

The sample is written in C#.

1. Create a new Console solution in Visual Studio.
2. Replace Program.cs with the corresponding code below.
3. Replace the `endpoint` value with the URI as explained in the [Variations](#) section.
4. Replace the `subscriptionKey` value with the key value that you retrieved above.
5. Replace the `region` value with the region value where you created your translator resource.
6. Replace the `text` value with text that you want to translate.
7. Run the program.

You can also test out different languages and texts by replacing the `text`, `from`, and `to` variables in Program.cs.

```
C#  
  
using System;  
using System.Collections.Generic;  
using Microsoft.Rest;  
using System.Net.Http;  
using System.Threading;  
using System.Threading.Tasks;  
using System.Net;  
using System.IO;  
using Newtonsoft.Json;  
using System.Text;  
  
namespace TextTranslator  
{  
    class Program  
    {  
        static string host = "PASTE ENDPOINT HERE";  
        static string path = "/translate?api-version=3.0";  
        // Translate to German.
```

```
static string params_ = "&to=de";  
  
static string uri = host + path + params_;  
  
// NOTE: Replace this example key with a valid subscription key.  
static string key = "PASTE KEY HERE";  
  
// NOTE: Replace this example region with a valid region.  
static string region = "PASTE REGION HERE";  
  
static string text = "Hello world!";  
  
async static void Translate()  
{  
    System.Object[] body = new System.Object[] { new { Text = text } };  
  
    var requestBody = JsonConvert.SerializeObject(body);  
  
    using (var client = new HttpClient())  
    using (var request = new HttpRequestMessage())  
    {  
        request.Method = HttpMethod.Post;  
        request.RequestUri = new Uri(uri);  
        request.Content = new StringContent(requestBody,  
Encoding.UTF8, "application/json");  
        request.Headers.Add("Ocp-Apim-Subscription-Key", key);  
        request.Headers.Add("Ocp-Apim-Subscription-Region", region);  
  
        var response = await client.SendAsync(request);  
        var responseBody = await  
response.Content.ReadAsStringAsync();  
        var result =  
JsonConvert.SerializeObject(JsonConvert.DeserializeObject(responseBody),  
Formatting.Indented);  
  
        Console.OutputEncoding = UnicodeEncoding.UTF8;  
        Console.WriteLine(result);  
    }  
}  
  
static void Main(string[] args)  
{  
    Translate();  
    Console.ReadLine();  
}  
}
```

For more information, see [public documentation](#) and [public API documentation](#) for Translator.

Next Steps

- Subscribe to the [Azure Government blog](#)
- Get help on Stack Overflow by using the "[azure-gov](#)" tag

Develop with SQL Server Management Studio

Article • 04/25/2022

To use SQL Server Management Studio (SSMS) with Azure Government, specify Azure Government as the environment to connect to, rather than global Azure. To connect to computers that are running SQL Server in your Azure Government subscription, you must configure SSMS to connect to the Azure Government cloud.

For general information about SSMS, see the [SSMS documentation](#).

If you don't have an Azure Government subscription, create a [free account](#) before you begin.

Prerequisites

- Review [Guidance for developers](#). This article discusses Azure Government's unique URLs and endpoints for managing your environment. You must know about these endpoints in order to connect to Azure Government.
- Review [Compare Azure Government and global Azure](#) and click on a service of interest to see variations between Azure Government and global Azure.

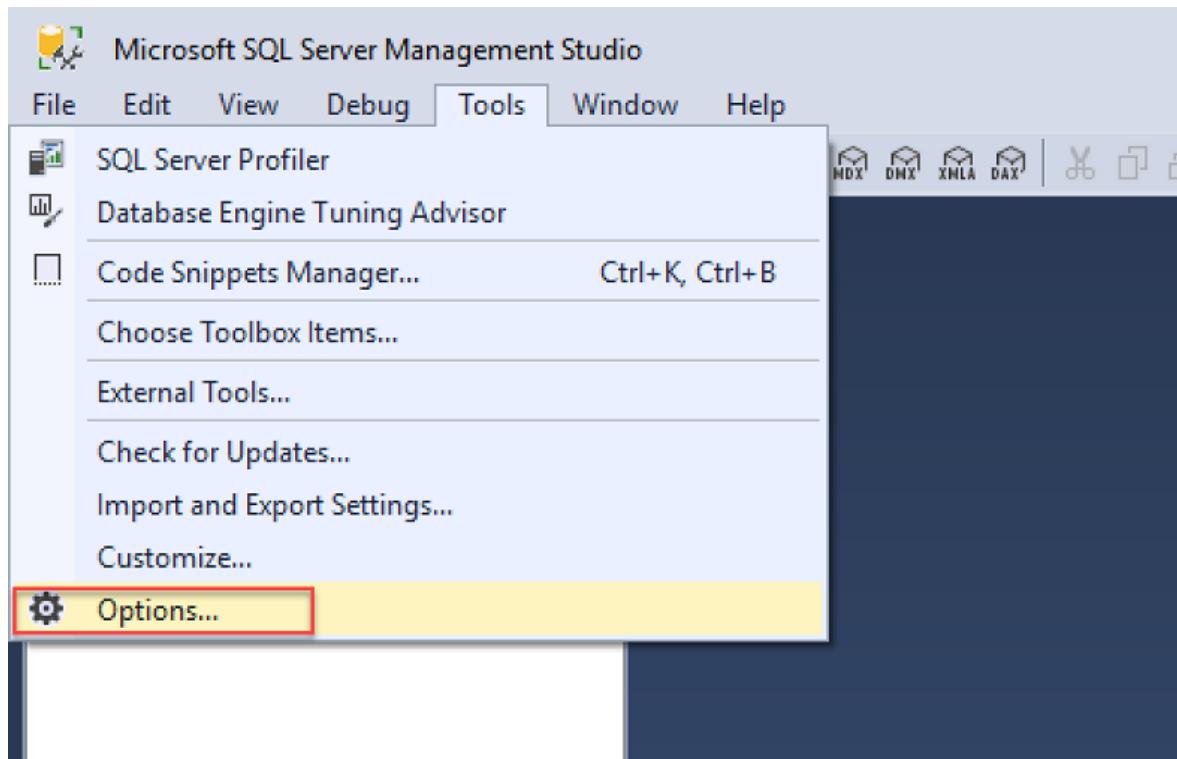
Set up an Azure SQL Server firewall rule

Before you connect to Azure Government from SSMS, you must set up an Azure SQL Server firewall rule to allow your local IP address to access your computer that's running SQL Server.

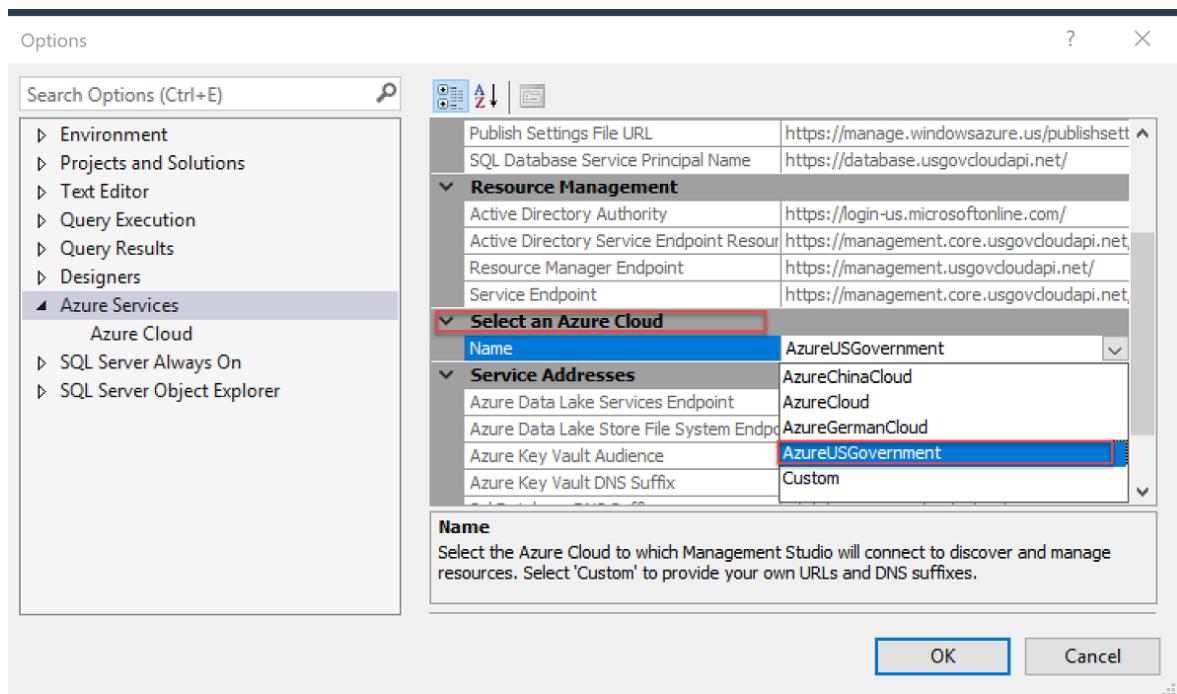
Follow these steps to [Manage firewall rules by using the Azure portal](#).

Specify Azure Government as the environment to connect

1. Open SSMS. Browse to **Tools > Options > Azure Services**.



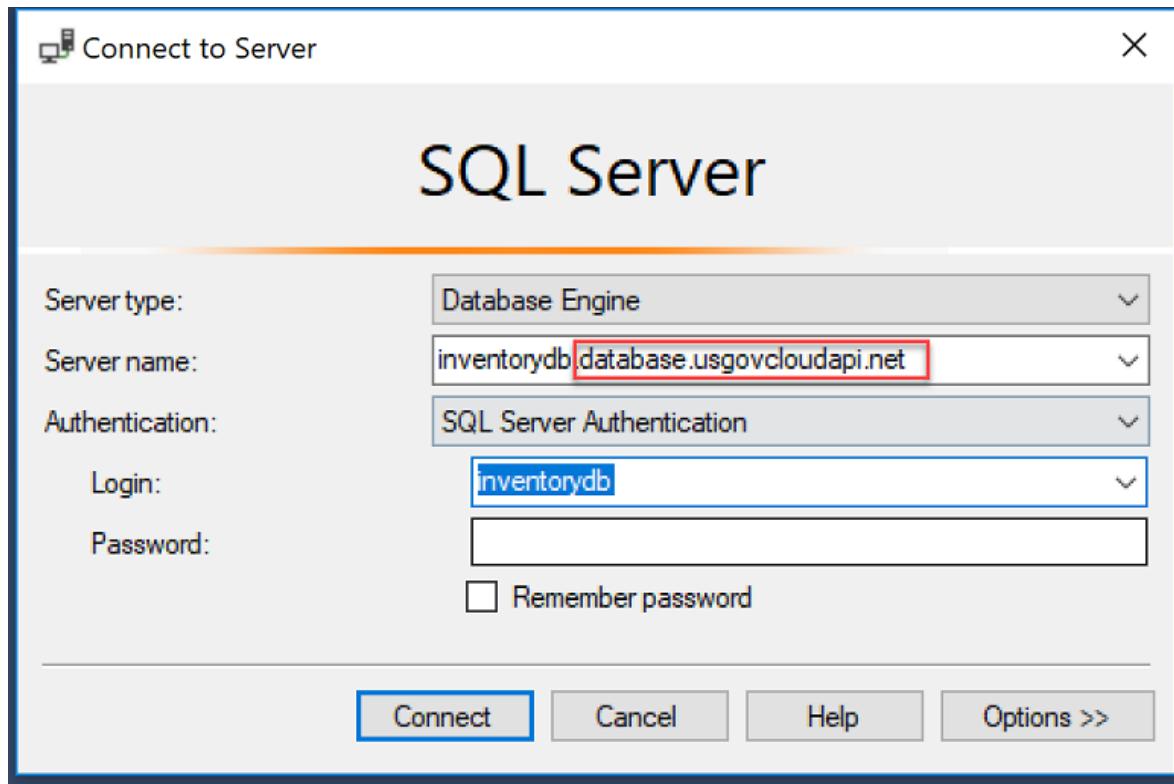
2. In the Select an Azure Cloud drop-down, select **AzureUSGovernment**.



3. Browse to **File > Connect Object Explorer**. Enter the name of your computer that's running SQL Server. Enter your authentication information.

➊ Note

The name of the computer that's running SQL Server ends with **.usgovcloudapi.net**.



SSMS is now connected to your Azure Government subscription.

Next steps

- Read more about [Azure Storage](#).
- Subscribe to the [Azure Government blog ↗](#).
- Get help on Stack Overflow by using the [azure-gov ↗](#) tag.

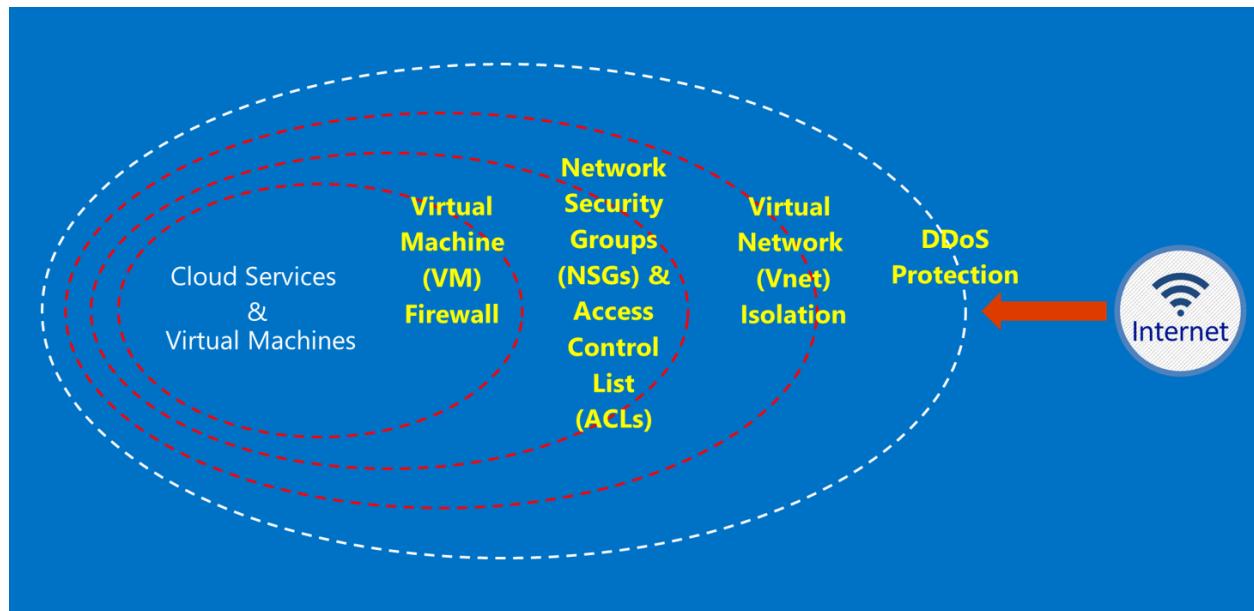
Azure Government security

Article • 03/22/2022

Azure Government provides a range of features and services that you can use to build cloud solutions to meet your regulated/controlled data needs. A compliant customer solution can be a combination of the effective implementation of out-of-the-box Azure Government capabilities coupled with a solid data security practice.

When you host a solution in Azure Government, Microsoft handles many of these requirements at the cloud infrastructure level.

The following diagram shows the Azure defense-in-depth model. For example, Microsoft provides basic cloud infrastructure Distributed Denial of Service (DDoS) protection, along with customer capabilities such as [Azure DDoS Protection](#) or security appliances for customer-specific application DDoS needs.



This article outlines the foundational principles for securing your services and applications. It provides guidance and best practices on how to apply these principles. For example, how you should make smart use of Azure Government to meet requirements for a solution that handles information subject to the [International Traffic in Arms Regulations](#) (ITAR). For extra security recommendations and implementation details to help you improve your security posture with respect to Azure resources, see the [Azure Security Benchmark](#).

The overarching principles for securing customer data are:

- Protecting data using encryption
- Managing secrets
- Isolation to restrict data access

These principles are applicable to both Azure and Azure Government. As described in [Understanding isolation](#), Azure Government provides extra physical networking isolation and meets demanding US government compliance requirements.

Data encryption

Mitigating risk and meeting regulatory obligations are driving the increasing focus and importance of data encryption. Use an effective encryption implementation to enhance current network and application security measures and decrease the overall risk of your cloud environment. Azure has extensive support to safeguard customer data using [data encryption](#), including various encryption models:

- Server-side encryption that uses service-managed keys, customer-managed keys (CMK) in Azure, or CMK in customer-controlled hardware.
- Client-side encryption that enables you to manage and store keys on-premises or in another secure location. Client-side encryption is built into the Java and .NET storage client libraries, which can use Azure Key Vault APIs, making the implementation straightforward. You can use Microsoft Entra ID to provide specific individuals with access to Azure Key Vault secrets.

Data encryption provides isolation assurances that are tied directly to encryption key access. Since Azure uses strong ciphers for data encryption, only entities with access to encryption keys can have access to data. Deleting or revoking encryption keys renders the corresponding data inaccessible.

Encryption at rest

Azure provides extensive options for [encrypting data at rest](#) to help you safeguard your data and meet your compliance needs using both Microsoft-managed encryption keys and customer-managed encryption keys. This process relies on multiple encryption keys and services such as Azure Key Vault and Microsoft Entra ID to ensure secure key access and centralized key management. For more information about Azure Storage service encryption and Azure disk encryption, see [Data encryption at rest](#).

Encryption in transit

Azure provides many options for [encrypting data in transit](#). Data encryption in transit isolates your network traffic from other traffic and helps protect data from interception. For more information, see [Data encryption in transit](#).

The basic encryption available for connectivity to Azure Government supports Transport Layer Security (TLS) 1.2 protocol and X.509 certificates. Federal Information Processing Standard (FIPS) 140 validated cryptographic algorithms are also used for infrastructure network connections between Azure Government datacenters. Windows, Windows Server, and Azure File shares can use SMB 3.0 for encryption between the virtual machine (VM) and the file share. Use client-side encryption to encrypt the data before it's transferred into storage in a client application, and to decrypt the data after it's transferred out of storage.

Best practices for encryption

- **IaaS VMs:** Use Azure disk encryption. Turn on Storage service encryption to encrypt the VHD files that are used to back up those disks in Azure Storage. This approach only encrypts newly written data. If you create a VM and then enable Storage service encryption on the storage account that holds the VHD file, only the changes will be encrypted, not the original VHD file.
- **Client-side encryption:** Represents the most secure method for encrypting your data, because it encrypts it before transit, and encrypts the data at rest. However, it does require that you add code to your applications using storage, which you might not want to do. In those cases, you can use HTTPS for your data in transit, and Storage service encryption to encrypt the data at rest. Client-side encryption also involves more load on the client that you have to account for in your scalability plans, especially if you're encrypting and transferring much data.

Managing secrets

Proper protection and management of encryption keys is essential for data security. You should strive to simplify key management and maintain control of keys used by cloud applications and services to encrypt data. [Azure Key Vault](#) is a cloud service for securely storing and managing secrets. Key Vault enables you to store your encryption keys in hardware security modules (HSMs) that are [FIPS 140](#) validated. For more information, see [Data encryption key management](#).

Best practices for managing secrets

- Use Key Vault to minimize the risks of secrets being exposed through hard-coded configuration files, scripts, or in source code. For added assurance, you can import or generate keys in Azure Key Vault HSMs.
- Application code and templates should only contain URI references to the secrets, meaning the actual secrets aren't in code, configuration, or source code

repositories. This approach prevents key phishing attacks on internal or external repositories, such as harvest-bots at GitHub.

- Utilize strong Azure role-based access control (RBAC) within Key Vault. A trusted operator who leaves the company or transfers to a new group within the company should be prevented from being able to access the secrets.

Understanding isolation

Isolation in Azure Government is achieved through the implementation of trust boundaries, segmentation, and containers to limit data access only to authorized users, services, and applications. Azure Government supports environment and tenant isolation controls and capabilities.

Environment isolation

The Azure Government multi-tenant cloud platform environment is an Internet standards-based Autonomous System (AS) that is physically isolated and separately administered from the rest of Azure public cloud. As defined by [IETF RFC 4271](#), the AS is composed of a set of switches and routers under a single technical administration, using an interior gateway protocol and common metrics to route packets within the AS. An exterior gateway protocol is used to route packets to other ASs through a single and clearly defined routing policy.

The isolation of the Azure Government environment is achieved through a series of physical and logical controls that include:

- Physically isolated hardware
- Physical barriers to the hardware using biometric devices and cameras
- Conditional access (Azure RBAC, workflow)
- Specific credentials and multi-factor authentication for logical access
- Infrastructure for Azure Government is located within the United States

Within the Azure Government network, internal network system components are isolated from other system components through implementation of separate subnets and access control policies on management interfaces. Azure Government doesn't directly peer with the public internet or with the Microsoft corporate network. Azure Government directly peers to the commercial Microsoft Azure network, which has routing and transport capabilities to the Internet and the Microsoft Corporate network. Azure Government limits its exposed surface area by applying extra protections and communications capabilities of our commercial Azure network. In addition, Azure Government ExpressRoute (ER) uses peering with our customer's networks over non-

Internet private circuits to route ER customer “DMZ” networks using specific Border Gateway Protocol (BGP)/AS peering as a trust boundary for application routing and associated policy enforcement.

Azure Government maintains the following authorizations:

- FedRAMP High provisional authorization to operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB)
- DoD SRG IL4 and IL5 provisional authorizations (PA) issued by the Defense Information Systems Agency (DISA)

Tenant isolation

Separation between customers/tenants is an essential security mechanism for both Azure and Azure Government multi-tenant cloud environments. Azure and Azure Government provide baseline per-customer or tenant isolation controls including isolation of Hypervisor, Root OS, and Guest VMs, isolation of Fabric Controllers, packet filtering, and VLAN isolation. For more information, see [Compute isolation](#).

You can manage your isolation posture to meet individual requirements through network access control and segregation through virtual machines, virtual networks, VLAN isolation, ACLs, load balancers, and IP filters. Additionally, you can further manage isolation levels for your resources across subscriptions, resource groups, virtual networks, and subnets. The customer/tenant logical isolation controls help prevent one tenant from interfering with the operations of any other customer/tenant.

Screening

All Azure and Azure Government employees in the United States are subject to Microsoft background checks. Personnel with the ability to access customer data for troubleshooting purposes in Azure Government are additionally subject to the verification of US citizenship and extra screening requirements where appropriate.

We're now screening all our operators at a Tier 3 Investigation (formerly National Agency Check with Law and Credit, NACLC) as defined in Section 5.6.2.2 (Page 77) of the DoD [Cloud Computing SRG](#):

Note

The minimum background investigation required for CSP personnel having access to Level 4 and 5 information based on a “noncritical-sensitive” (e.g., DoD’s ADP-2)

is a Tier 3 Investigation (for “noncritical-sensitive” contractors), or a Moderate Risk Background Investigation (MBI) for a “moderate risk” position designation.

[+] [Expand table](#)

Applicable screening and background check	Environment	Frequency	Description
New hire check	Azure Azure Gov	Upon employment	<ul style="list-style-type: none"> - Education history (highest degree) - Employment history (7-yr history) - Social Security Number search - Criminal history check (7-yr history) - Office of Foreign Assets Control (OFAC) list - Bureau of Industry and Security (BIS) list - Office of Defense Trade Controls (DDTC) debarred list
Cloud screen	Azure Azure Gov	Every two years	<ul style="list-style-type: none"> - Social Security Number search - Criminal history check (7-yr history) - Office of Foreign Assets Control (OFAC) list - Bureau of Industry and Security (BIS) list - Office of Defense Trade Controls (DDTC) debarred list
US citizenship	Azure Gov	Upon employment	<ul style="list-style-type: none"> - Verification of US citizenship
Criminal Justice Information Services (CJIS)	Azure Gov	Upon signed CJIS agreement with State	<ul style="list-style-type: none"> - Adds fingerprint background check against FBI database - Criminal records check and credit check
Tier 3 Investigation	Azure Gov	Upon signed contract with sponsoring agency	<ul style="list-style-type: none"> - Detailed background and criminal history investigation (SF 86)

For Azure operations personnel, the following access principles apply:

- Duties are clearly defined, with separate responsibilities for requesting, approving, and deploying changes.
- Access is through defined interfaces that have specific functionality.
- Access is just-in-time (JIT), and is granted on a per-incident basis or for a specific maintenance event, and for a limited duration.
- Access is rule-based, with defined roles that are only assigned the permissions required for troubleshooting.

Screening standards include the validation of US citizenship of all Microsoft support and operational staff before access is granted to Azure Government-hosted systems.

Support personnel who need to transfer data use the secure capabilities within Azure Government. Secure data transfer requires a separate set of authentication credentials to gain access.

Restrictions on insider access

Controls for restricting insider access to customer data are the same for both Azure and Azure Government. As described in the previous section, Azure Government imposes extra personnel background screening requirements, including verification of US citizenship.

Note

Insider threat is characterized as potential for providing back-door connections and cloud service provider (CSP) privileged administrator access to customer's systems and data. Microsoft provides strong [customer commitments](#) regarding who can access customer data and on what terms. Access to customer data by Microsoft operations and support personnel is **denied by default**. Access to customer data isn't needed to operate Azure. Moreover, for most support scenarios involving customer troubleshooting tickets, access to customer data isn't needed.

No default access rights and Just-in-Time (JIT) access provisions reduce greatly the risks associated with traditional on-premises administrator elevated access rights that typically persist throughout the duration of employment. Microsoft makes it considerably more difficult for malicious insiders to tamper with your applications and data. The same access control restrictions and processes are imposed on all Microsoft engineers, including both full-time employees and subprocessors/vendors. The following controls are in place to restrict insider access to your data:

- Internal Microsoft controls that prevent access to production systems unless it's authorized through **Just-in-Time (JIT)** privileged access management system, as described in this section.
- Enforcement of **Customer Lockbox** that puts you in charge of approving insider access in support and troubleshooting scenarios, as described in this section. For most support scenarios, access to your data isn't required.
- **Data encryption** with option for customer-managed encryption keys – encrypted data is accessible only by entities who are in possession of the key, as described previously.
- **Customer monitoring** of external access to provisioned Azure resources, which includes security alerts as described in the next section.

Access control requirements

Microsoft takes strong measures to protect your data from inappropriate access or use by unauthorized persons. Microsoft engineers (including full-time employees and subprocessors/vendors) [don't have default access](#) to your data in the cloud. Instead, they're granted access, under management oversight, only when necessary. Using the [restricted access workflow](#), access to your data is carefully controlled, logged, and revoked when it's no longer needed. For example, access to your data may be required to resolve troubleshooting requests that you initiated. The access control requirements are [established by the following policy](#):

- No access to customer data, by default.
- No user or administrator accounts on customer virtual machines (VMs).
- Grant the least privilege that is required to complete task, audit, and log access requests.

Microsoft engineers can be granted access to customer data using temporary credentials via **Just-in-Time (JIT)** access. There must be an incident logged in the Azure Incident Management system that describes the reason for access, approval record, what data was accessed, etc. This approach ensures that there's appropriate oversight for all access to customer data and that all JIT actions (consent and access) are logged for audit. Evidence that procedures have been established for granting temporary access for Azure personnel to customer data and applications upon appropriate approval for customer support or incident handling purposes is available from the Azure [SOC 2 Type 2 attestation report](#) produced by an independent third-party auditing firm.

JIT access works with multi-factor authentication that requires Microsoft engineers to use a smartcard to confirm their identity. All access to production systems is performed using Secure Admin Workstations (SAWs) that are consistent with published guidance on securing privileged access. Use of SAWs for access to production systems is required

by Microsoft policy and compliance with this policy is closely monitored. These workstations use a fixed image with all software fully managed – only select activities are allowed and users cannot accidentally circumvent the SAW design since they don't have admin privileges on these machines. Access is permitted only with a smartcard and access to each SAW is limited to specific set of users.

Customer Lockbox

[Customer Lockbox for Azure](#) is a service that provides you with the capability to control how a Microsoft engineer accesses your data. As part of the support workflow, a Microsoft engineer may require elevated access to your data. Customer Lockbox puts you in charge of that decision by enabling you to approve/deny such elevated requests. Customer Lockbox is an extension of the JIT workflow and comes with full audit logging enabled. Customer Lockbox capability isn't required for support cases that don't involve access to customer data. For most support scenarios, access to customer data isn't needed and the workflow shouldn't require Customer Lockbox. Microsoft engineers rely heavily on logs to maintain Azure services and provide customer support.

Customer Lockbox is available to all customers who have an Azure support plan with a minimum level of Developer. You can enable Customer Lockbox from the [Administration module](#) in the Customer Lockbox blade. A Microsoft engineer will initiate Customer Lockbox request if this action is needed to progress a customer-initiated support ticket. Customer Lockbox is available to customers from all Azure public regions.

Guest VM memory crash dumps

On each Azure node, there's a Hypervisor that runs directly over the hardware and divides the node into a variable number of Guest virtual machines (VMs), as described in [Compute isolation](#). Each node also has one special Root VM, which runs the Host OS.

When a Guest VM (also known as customer VM) crashes, customer data may be contained inside a memory dump file on the Guest VM. **By default, Microsoft engineers don't have access to Guest VMs and can't review crash dumps on Guest VMs without customer's approval.** The same process involving explicit customer authorization is used to control access to Guest VM crash dumps should you request an investigation of your VM crash. As described previously, access is gated by the JIT privileged access management system and Customer Lockbox so that all actions are logged and audited. The primary forcing function for deleting the memory dumps from Guest VMs is the routine process of VM reimaging that typically occurs at least every two months.

Data deletion, retention, and destruction

As a customer, you're [always in control of your customer data](#) in Azure. You can access, extract, and delete your customer data stored in Azure at will. When you terminate your Azure subscription, Microsoft takes the necessary steps to ensure that you continue to own your customer data. A common customer concern upon data deletion or subscription termination is whether another customer or Azure administrator can access their deleted data. For more information on how data deletion, retention, and destruction are implemented in Azure, see our online documentation:

- [Data deletion](#)
- [Data retention](#)
- [Data destruction](#)

Customer monitoring of Azure resources

This section covers essential Azure services that you can use to gain in-depth insight into your provisioned Azure resources and get alerted about suspicious activity, including outside attacks aimed at your applications and data. For a complete list, see the Azure service directory sections for [Management + Governance](#), [Networking](#), and [Security](#). Moreover, the [Azure Security Benchmark](#) provides security recommendations and implementation details to help you improve your security posture with respect to Azure resources.

[Microsoft Defender for Cloud](#) (formerly Azure Security Center) provides unified security management and advanced threat protection across hybrid cloud workloads. It's an essential service for you to limit your exposure to threats, protect cloud resources, [respond to incidents](#), and improve your regulatory compliance posture.

With Microsoft Defender for Cloud, you can:

- Monitor security across on-premises and cloud workloads.
- Apply advanced analytics and threat intelligence to detect attacks.
- Use access and application controls to block malicious activity.
- Find and fix vulnerabilities before they can be exploited.
- Simplify investigation when responding to threats.
- Apply policy to ensure compliance with security standards.

To assist you with Microsoft Defender for Cloud usage, Microsoft has published extensive [online documentation](#) and numerous blog posts covering specific security topics:

- [How Microsoft Defender for Cloud detects a Bitcoin mining attack](#)

- How Microsoft Defender for Cloud detects DDoS attack using cyber threat intelligence ↗
- How Microsoft Defender for Cloud aids in detecting good applications being used maliciously ↗
- How Microsoft Defender for Cloud unveils suspicious PowerShell attack ↗
- How Microsoft Defender for Cloud helps reveal a cyber attack ↗
- How Microsoft Defender for Cloud helps analyze attacks using Investigation and Log Search ↗
- Microsoft Defender for Cloud adds context alerts to aid threat investigation ↗
- How Microsoft Defender for Cloud automates the detection of cyber attack ↗
- Heuristic DNS detections in Microsoft Defender for Cloud ↗
- Detect the latest ransomware threat (Bad Rabbit) with Microsoft Defender for Cloud ↗
- Petya ransomware prevention & detection in Microsoft Defender for Cloud ↗
- Detecting in-memory attacks with Sysmon and Microsoft Defender for Cloud ↗
- How Defender for Cloud and Log Analytics can be used for threat hunting ↗
- How Microsoft Defender for Cloud helps detect attacks against your Linux machines ↗
- Use Microsoft Defender for Cloud to detect when compromised Linux machines attack ↗

Azure Monitor helps you maximize the availability and performance of applications by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from both cloud and on-premises environments. It helps you understand how your applications are performing, and proactively identifies issues affecting deployed applications and resources they depend on. Azure Monitor integrates the capabilities of [Log Analytics](#) and [Application Insights](#) that were previously branded as standalone services.

Azure Monitor collects data from each of the following tiers:

- **Application monitoring data:** Data about the performance and functionality of the code you've written, regardless of its platform.
- **Guest OS monitoring data:** Data about the operating system on which your application is running. The application could be running in Azure, another cloud, or on-premises.
- **Azure resource monitoring data:** Data about the operation of an Azure resource.
- **Azure subscription monitoring data:** Data about the operation and management of an Azure subscription and data about the health and operation of Azure itself.
- **Azure tenant monitoring data:** Data about the operation of tenant-level Azure services, such as Microsoft Entra ID.

With Azure Monitor, you can get a 360-degree view of your applications, infrastructure, and network with advanced analytics, dashboards, and visualization maps. Azure Monitor provides intelligent insights and enables better decisions with AI. You can analyze, correlate, and monitor data from various sources using a powerful query language and built-in machine learning constructs. Moreover, Azure Monitor provides out-of-the-box integration with popular DevOps, IT Service Management (ITSM), and Security Information and Event Management (SIEM) tools.

[Azure Policy](#) enables effective governance of Azure resources by creating, assigning, and managing policies. These policies enforce various rules over provisioned Azure resources to keep them compliant with your specific corporate security and privacy standards. For example, one of the built-in policies for Allowed Locations can be used to restrict available locations for new resources to enforce your geo-compliance requirements. For additional customer assistance, Microsoft provides **Azure Policy regulatory compliance built-in initiatives**, which map to **compliance domains** and **controls** in many US government, global, regional, and industry standards. For more information, see [Azure Policy samples](#). Regulatory compliance in Azure Policy provides built-in initiative definitions to view a list of the controls and compliance domains based on responsibility – customer, Microsoft, or shared. For Microsoft-responsible controls, we provide additional audit result details based on third-party attestations and our control implementation details to achieve that compliance. Each 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.

[Azure Firewall](#) provides a managed, cloud-based network security service that protects your Azure Virtual Network resources. It's a fully stateful firewall as a service with built-in high availability that integrates with Azure Monitor for logging and analytics.

[Network Watcher](#) allows you to monitor, diagnose, and gain insights into your Azure Virtual Network performance and health. With network security group flow logs, you can gain deeper understanding of your network traffic patterns and collect data for compliance, auditing, and monitoring of your network security profile. Packet capture allows you to capture traffic to and from your virtual machines to diagnose network anomalies and gather network statistics, including information on network intrusions.

[Azure DDoS Protection](#) provides extensive Distributed Denial of Service (DDoS) mitigation capability to help you protect your Azure resources from attacks. Always-on traffic monitoring provides near real-time detection of a DDoS attack, with automatic

mitigation of the attack as soon as it's detected. In combination with Web Application Firewall, DDoS Protection defends against a comprehensive set of network layer attacks, including SQL injection, cross-site scripting attacks, and session hijacks. Azure DDoS Protection is integrated with Azure Monitor for analytics and insight.

Microsoft Sentinel (formerly Azure Sentinel) is a cloud-native SIEM platform that uses built-in AI to help you quickly analyze large volumes of data across an enterprise. Microsoft Sentinel aggregates data from various sources, including users, applications, servers, and devices running on-premises or in any cloud, letting you reason over millions of records in a few seconds. With Microsoft Sentinel, you can:

- **Collect** data at cloud scale across all users, devices, applications, and infrastructure, both on-premises and in multiple clouds.
- **Detect** previously uncovered threats and minimize false positives using analytics and unparalleled threat intelligence from Microsoft.
- **Investigate** threats with AI and hunt suspicious activities at scale, tapping into decades of cybersecurity work at Microsoft.
- **Respond** to incidents rapidly with built-in orchestration and automation of common tasks.

Azure Advisor helps you follow best practices to optimize your Azure deployments. It analyzes resource configurations and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of Azure resources.

Next steps

- [Azure Government overview](#)
- [Azure Government compliance](#)
- [Azure and other Microsoft services compliance offerings](#)
- [Compare Azure Government and global Azure](#)
- [Azure guidance for secure isolation](#)
- [Azure Government isolation guidelines for Impact Level 5 workloads](#)
- [Azure Government DoD overview](#)
- [Azure security fundamentals documentation](#)
- [Azure Policy regulatory compliance built-in initiatives](#)

Isolation guidelines for Impact Level 5 workloads

Article • 01/04/2024

Azure Government supports applications that use Impact Level 5 (IL5) data in all available regions. IL5 requirements are defined in the [US Department of Defense \(DoD\) Cloud Computing Security Requirements Guide \(SRG\)](#). IL5 workloads have a higher degree of impact to the DoD and must be secured to a higher standard. When you deploy these workloads on Azure Government, you can meet their isolation requirements in various ways. The guidance in this document addresses configurations and settings needed to meet the IL5 isolation requirements. We'll update this article as we enable new isolation options and the Defense Information Systems Agency (DISA) authorizes new services for IL5 data.

Background

In January 2017, DISA awarded the [IL5 Provisional Authorization \(PA\)](#) to [Azure Government](#), making it the first IL5 PA awarded to a hyperscale cloud provider. The PA covered two Azure Government regions US DoD Central and US DoD East (US DoD regions) that are [dedicated to the DoD](#). Based on DoD mission owner feedback and evolving security capabilities, Microsoft has partnered with DISA to expand the IL5 PA boundary in December 2018 to cover the remaining Azure Government regions US Gov Arizona, US Gov Texas, and US Gov Virginia (US Gov regions). For service availability in Azure Government, see [Products available by region](#).

- For a list of services in scope for DoD IL5 PA in US Gov regions, see [Azure Government services by audit scope](#).
- For a list of services in scope for DoD IL5 PA in US DoD regions, see [Azure Government DoD regions IL5 audit scope](#).

Azure Government is available to US federal, state, local, and tribal governments and their partners. The IL5 expansion to Azure Government honors the isolation requirements mandated by the DoD. Azure Government continues to provide more PaaS services suitable for DoD IL5 workloads than any other cloud services environment.

Principles and approach

You need to address two key areas for Azure services in IL5 scope: compute isolation and storage isolation. We'll focus in this article on how Azure services can help you

isolate the compute and storage services for IL5 data. The SRG allows for a shared management and network infrastructure. **This article is focused on Azure Government compute and storage isolation approaches for US Gov Arizona, US Gov Texas, and US Gov Virginia regions (US Gov regions).** If an Azure service is available in Azure Government DoD regions US DoD Central and US DoD East (US DoD regions) and authorized at IL5, then it is by default suitable for IL5 workloads with no extra isolation configuration required. Azure Government DoD regions are reserved for DoD agencies and their partners, enabling physical separation from non-DoD tenants by design. For more information, see [DoD in Azure Government](#).

Important

You are responsible for designing and deploying your applications to meet DoD IL5 compliance requirements. In doing so, you should not include sensitive or restricted information in Azure resource names, as explained in [Considerations for naming Azure resources](#).

Compute isolation

IL5 separation requirements are stated in Section 5.2.2.3 (Page 51) of the [Cloud Computing SRG](#). The SRG focuses on compute separation during "processing" of IL5 data. This separation ensures that a virtual machine that could potentially compromise the physical host can't affect a DoD workload. To remove the risk of runtime attacks and ensure long running workloads aren't compromised from other workloads on the same host, **all IL5 virtual machines and virtual machine scale sets** should be isolated by DoD mission owners via [Azure Dedicated Host](#) or [isolated virtual machines](#). Doing so provides a dedicated physical server to host your Azure Virtual Machines (VMs) for Windows and Linux.

For services where the compute processes are obfuscated from access by the owner and stateless in their processing of data, you should accomplish isolation by focusing on the data being processed and how it's stored and retained. This approach ensures the data is stored in protected mediums. It also ensures the data isn't present on these services for extended periods unless it's encrypted as needed.

Storage isolation

The DoD requirements for encrypting data at rest are provided in Section 5.11 (Page 122) of the [Cloud Computing SRG](#). DoD emphasizes encrypting all data at rest stored in virtual machine virtual hard drives, mass storage facilities at the block or file level, and

database records where the mission owner doesn't have sole control over the database service. For cloud applications where encrypting data at rest with DoD key control isn't possible, mission owners must perform a risk analysis with relevant data owners before transmitting data into a cloud service offering.

In a recent PA for Azure Government, DISA approved logical separation of IL5 from other data via cryptographic means. In Azure, this approach involves data encryption via keys that are maintained in Azure Key Vault and stored in [FIPS 140 validated](#) Hardware Security Modules (HSMs). The keys are owned and managed by the IL5 system owner, also known as customer-managed keys (CMK).

Here's how this approach applies to services:

- If a service hosts only IL5 data, the service can control the key for end users. But it must use a dedicated key to protect IL5 data from all other data in the cloud.
- If a service will host IL5 and non-DoD data, the service must expose the option for end users to use their own encryption keys that are maintained in Azure Key Vault. This implementation gives consumers of the service the ability to implement cryptographic separation as needed.

This approach ensures all key material for decrypting data is stored separately from the data itself using a hardware-based key management solution.

Applying this guidance

IL5 guidelines require workloads to be deployed with a high degree of security, isolation, and control. The following configurations are required *in addition* to any other configurations or controls needed to meet IL5 requirements. Network isolation, access controls, and other necessary security measures aren't necessarily addressed in this article.

Note

This article tracks Azure services that have received DoD IL5 PA and that require extra configuration options to meet IL5 isolation requirements. Services with IL5 PA that do not require any extra configuration options are not mentioned in this article. For a list of services in scope for DoD IL5 PA in US Gov regions, see [Azure Government services by audit scope](#).

Be sure to review the entry for each service you're using and ensure that all isolation requirements are implemented.

AI + machine learning

For AI and machine learning services availability in Azure Government, see [Products available by region](#). For a list of services in scope for DoD IL5 PA, see [Azure Government services by audit scope](#). Guidance below is provided only for IL5 PA services that require extra configuration to support IL5 workloads.

Azure AI Search

- Configure encryption at rest of content in Azure AI Search by [using customer-managed keys in Azure Key Vault](#).

Azure Machine Learning

- Configure encryption at rest of content in Azure Machine Learning by using customer-managed keys in Azure Key Vault. Azure Machine Learning stores snapshots, output, and logs in the Azure Blob Storage account that's associated with the Azure Machine Learning workspace and customer subscription. All the data stored in Azure Blob Storage is [encrypted at rest with Microsoft-managed keys](#). Customers can use their own keys for data stored in Azure Blob Storage. See [Configure encryption with customer-managed keys stored in Azure Key Vault](#).

Azure AI services: Content Moderator

- Configure encryption at rest of content in the Content Moderator service by [using customer-managed keys in Azure Key Vault](#).

Azure AI services: Custom Vision

- Configure encryption at rest of content in Azure AI Custom Vision [using customer-managed keys in Azure Key Vault](#).

Azure AI services: Face

- Configure encryption at rest of content in the Face service by [using customer-managed keys in Azure Key Vault](#).

Azure AI Language Understanding (LUIS)

- Configure encryption at rest of content in the Language Understanding service by using [customer-managed keys in Azure Key Vault](#).

Azure AI Language Understanding (LUIS) is part of [Azure AI Language](#).

Azure AI services: Personalizer

- Configure encryption at rest of content in Azure AI Personalizer [using customer-managed keys in Azure Key Vault](#).

Azure AI services: QnA Maker

- Configure encryption at rest of content in Azure AI QnA Maker [using customer-managed keys in Azure Key Vault](#).

Azure AI QnA Maker is part of [Azure AI Language](#).

Azure AI Speech

- Configure encryption at rest of content in Speech Services by [using customer-managed keys in Azure Key Vault](#).

Azure AI services: Translator

- Configure encryption at rest of content in the Translator service by [using customer-managed keys in Azure Key Vault](#).

Analytics

For Analytics services availability in Azure Government, see [Products available by region](#). For a list of services in scope for DoD IL5 PA, see [Azure Government services by audit scope](#). Guidance below is provided only for IL5 PA services that require extra configuration to support IL5 workloads.

Azure Databricks

- Azure Databricks can be deployed to existing storage accounts that have enabled appropriate [Storage encryption with Key Vault managed keys](#).
- Configure customer-managed Keys (CMK) for your [Azure Databricks Workspace](#) and [Databricks File System](#) (DBFS).

Azure Data Explorer

- Data in Azure Data Explorer clusters in Azure is secured and encrypted with Microsoft-managed keys by default. For extra control over encryption keys, you can supply customer-managed keys to use for data encryption and manage encryption of your data at the storage level with your own keys.

Azure HDInsight

- Azure HDInsight can be deployed to existing storage accounts that have enabled appropriate [Storage service encryption](#), as discussed in the guidance for Azure Storage.
- Azure HDInsight enables a database option for certain configurations. Ensure the appropriate database configuration for transparent data encryption (TDE) is enabled on the option you choose. This process is discussed in the guidance for [Azure SQL Database](#).

Azure Stream Analytics

- Configure encryption at rest of content in Azure Stream Analytics by [using customer-managed keys in Azure Key Vault](#).

Azure Synapse Analytics

- Add transparent data encryption with customer-managed keys via Azure Key Vault. For more information, see [Azure SQL transparent data encryption](#). The instructions to enable this configuration for Azure Synapse Analytics are the same as the instructions to do so for Azure SQL Database.

Data Factory

- Secure data store credentials by storing encrypted credentials in a Data Factory managed store. Data Factory helps protect your data store credentials by encrypting them with certificates managed by Microsoft. For more information about Azure Storage security, see [Azure Storage security overview](#). You can also store the data store's credentials in Azure Key Vault. Data Factory retrieves the credentials during the execution of an activity. For more information, see [Store credentials in Azure Key Vault](#).

Event Hubs

- Configure encryption at rest of content in Azure Event Hubs by [using customer-managed keys in Azure Key Vault](#).

Power BI

- Configure encryption at rest of content in Power BI by [using customer-managed keys in Azure Key Vault](#).

Compute

For Compute services availability in Azure Government, see [Products available by region](#). For a list of services in scope for DoD IL5 PA, see [Azure Government services by audit scope](#). Guidance below is provided only for IL5 PA services that require extra configuration to support IL5 workloads.

Batch

- Enable user subscription mode, which will require a Key Vault instance for proper encryption and key storage. For more information, see the documentation on [batch account configurations](#).

Virtual machines and virtual machine scale sets

You can use Azure virtual machines with multiple deployment mediums. You can do so for single virtual machines and for virtual machines deployed via the Azure virtual machine scale sets feature.

All virtual machines should use Disk Encryption for virtual machines or Disk Encryption for virtual machine scale sets, or place virtual machine disks in a storage account that can hold Impact Level 5 data as described in the [Azure Storage section](#).

 **Important**

When you deploy VMs in Azure Government regions US Gov Arizona, US Gov Texas, and US Gov Virginia, you must use Azure Dedicated Host, as described in the next section.

Azure Dedicated Host

Azure Dedicated Host provides physical servers that can host one or more virtual machines and that are dedicated to one Azure subscription. Dedicated hosts are the same physical servers used in our datacenters, provided as a resource. You can provision dedicated hosts within a region, availability zone, and fault domain. You can then place VMs directly into your provisioned hosts, in whatever configuration meets your needs.

These VMs provide the necessary level of isolation required to support IL5 workloads when deployed outside of the dedicated DoD regions. When you use Dedicated Host, your Azure VMs are placed on an isolated and dedicated physical server that runs only your organization's workloads to meet compliance guidelines and standards.

Current Dedicated Host SKUs (VM series and Host Type) that offer the required compute isolation include SKUs in the VM families listed on the [Dedicated Host pricing page](#).

Isolated virtual machines

Virtual machine scale sets aren't currently supported on Azure Dedicated Host. But specific VM types, when deployed, consume the entire physical host for the VM. Isolated VM types can be deployed via virtual machine scale sets to provide proper compute isolation with all the benefits of virtual machine scale sets in place. When you configure your scale set, select the appropriate SKU. To encrypt the data at rest, see the next section for supportable encryption options.

Important

As new hardware generations become available, some VM types might require reconfiguration (scale up or migration to a new VM SKU) to ensure they remain on properly dedicated hardware. For more information, see [Virtual machine isolation in Azure](#).

Disk encryption for virtual machines

You can encrypt the storage that supports these virtual machines in one of two ways to support necessary encryption standards.

- Use Azure Disk Encryption to encrypt the drives by using dm-crypt (Linux) or BitLocker (Windows):
 - [Enable Azure Disk Encryption for Linux](#)
 - [Enable Azure Disk Encryption for Windows](#)
- Use Azure Storage service encryption for storage accounts with your own key to encrypt the storage account that holds the disks:

- Storage service encryption with customer-managed keys

Disk encryption for virtual machine scale sets

You can encrypt disks that support virtual machine scale sets by using Azure Disk Encryption:

- Encrypt disks in virtual machine scale sets

Containers

For Containers services availability in Azure Government, see [Products available by region](#). For a list of services in scope for DoD IL5 PA, see [Azure Government services by audit scope](#). Guidance below is provided only for IL5 PA services that require extra configuration to support IL5 workloads.

Azure Kubernetes Service

- Configure encryption at rest of content in AKS by [using customer-managed keys in Azure Key Vault](#).

Container Instances

- Azure Container Instances automatically encrypts data related to your containers when it's persisted in the cloud. Data in Container Instances is encrypted and decrypted with 256-bit AES encryption and enabled for all Container Instances deployments. You can rely on Microsoft-managed keys for the encryption of your container data, or you can manage the encryption by using your own keys. For more information, see [Encrypt deployment data](#).

Container Registry

- When you store images and other artifacts in a Container Registry, Azure automatically encrypts the registry content at rest by using service-managed keys. You can supplement the default encryption with an extra encryption layer by [using a key that you create and manage in Azure Key Vault](#).

Databases

For Databases services availability in Azure Government, see [Products available by region](#). For a list of services in scope for DoD IL5 PA, see [Azure Government services by audit scope](#). Guidance below is provided only for IL5 PA services that require extra configuration to support IL5 workloads.

Azure Cosmos DB

- Data stored in your Azure Cosmos DB account is automatically and seamlessly encrypted with keys managed by Microsoft (service-managed keys). Optionally, you can choose to add a second layer of encryption with keys you manage (customer-managed keys). For more information, see [Configure customer-managed keys for your Azure Cosmos DB account with Azure Key Vault](#).

Azure Database for MySQL

- Data encryption with customer-managed keys for Azure Database for MySQL enables you to bring your own key (BYOK) for data protection at rest. This encryption is set at the server level. For a given server, a customer-managed key, called the key encryption key (KEK), is used to encrypt the data encryption key (DEK) used by the service. For more information, see [Azure Database for MySQL data encryption with a customer-managed key](#).

Azure Database for PostgreSQL

- Data encryption with customer-managed keys for Azure Database for PostgreSQL Single Server is set at the server level. For a given server, a customer-managed key, called the key encryption key (KEK), is used to encrypt the data encryption key (DEK) used by the service. For more information, see [Azure Database for PostgreSQL Single Server data encryption with a customer-managed key](#).

Azure Healthcare APIs (formerly Azure API for FHIR)

Azure Healthcare APIs supports Impact Level 5 workloads in Azure Government with this configuration:

- Configure encryption at rest of content in Azure Healthcare APIs [using customer-managed keys in Azure Key Vault](#)

Azure SQL Database

- Add transparent data encryption with customer-managed keys via Azure Key Vault. For more information, see [Azure SQL transparent data encryption with customer-managed key](#).

SQL Server Stretch Database

- Add transparent data encryption with customer-managed keys via Azure Key Vault. For more information, see [Azure SQL transparent data encryption with customer-managed key](#).

Hybrid

Azure Stack Edge

- You can protect data at rest via storage accounts because your device is associated with a storage account that's used as a destination for your data in Azure. You can configure your storage account to use data encryption with customer-managed keys stored in Azure Key Vault. For more information, see [Protect data in storage accounts](#).

Integration

For Integration services availability in Azure Government, see [Products available by region](#). For a list of services in scope for DoD IL5 PA, see [Azure Government services by audit scope](#). Guidance below is provided only for IL5 PA services that require extra configuration to support IL5 workloads.

Service Bus

- Configure encryption of data at rest in Azure Service Bus by [using customer-managed keys in Azure Key Vault](#).

Internet of Things

For Internet of Things services availability in Azure Government, see [Products available by region](#). For a list of services in scope for DoD IL5 PA, see [Azure Government services by audit scope](#). Guidance below is provided only for IL5 PA services that require extra configuration to support IL5 workloads.

Azure IoT Hub

- IoT Hub supports encryption of data at rest with customer-managed keys, also known as *bring your own key* (BYOK). Azure IoT Hub provides encryption of data at rest and in transit. By default, Azure IoT Hub uses Microsoft-managed keys to encrypt the data. Customer-managed key support enables you to encrypt data at rest by using an [encryption key that you manage via Azure Key Vault](#).

Management and governance

For Management and governance services availability in Azure Government, see [Products available by region](#). For a list of services in scope for DoD IL5 PA, see [Azure Government services by audit scope](#).

Automation

- By default, your Azure Automation account uses Microsoft-managed keys. You can manage the encryption of secure assets for your Automation account by using your own keys. When you specify a customer-managed key at the level of the Automation account, that key is used to protect and control access to the account encryption key for the Automation account. For more information, see [Encryption of secure assets in Azure Automation](#).

Azure Managed Applications

- You can store your managed application definition in a storage account that you provide when you create the application. Doing so allows you to manage its location and access for your regulatory needs, including [storage encryption with customer-managed keys](#). For more information, see [Bring your own storage](#).

Azure Monitor

- By default, all data and saved queries are encrypted at rest using Microsoft-managed keys. Configure encryption at rest of your data in Azure Monitor [using customer-managed keys in Azure Key Vault](#).

Log Analytics

Log Analytics, which is a feature of Azure Monitor, is intended to be used for monitoring the health and status of services and infrastructure. The monitoring data and logs

primarily store [logs and metrics](#) that are service generated. When used in this primary capacity, Log Analytics supports Impact Level 5 workloads in Azure Government with no extra configuration required.

Log Analytics may also be used to ingest extra customer-provided logs. These logs may include data ingested as part of operating Microsoft Defender for Cloud or Microsoft Sentinel. If the ingested logs or the queries written against these logs are categorized as IL5 data, then you should configure customer-managed keys (CMK) for your Log Analytics workspaces and Application Insights components. Once configured, any data sent to your workspaces or components is encrypted with your Azure Key Vault key. For more information, see [Azure Monitor customer-managed keys](#).

Azure Site Recovery

- You can replicate Azure VMs with managed disks enabled for customer-managed keys from one Azure region to another. For more information, see [Replicate machines with customer-managed keys enabled disks](#).

Microsoft Intune

- Intune supports Impact Level 5 workloads in Azure Government with no extra configuration required. Line-of-business apps should be evaluated for IL5 restrictions prior to [uploading to Intune storage](#). While Intune does encrypt applications that are uploaded to the service for distribution, it doesn't support customer-managed keys.

Media

For Media services availability in Azure Government, see [Products available by region](#). For a list of services in scope for DoD IL5 PA, see [Azure Government services by audit scope](#). Guidance below is provided only for IL5 PA services that require extra configuration to support IL5 workloads.

Media Services

- Configure encryption at rest of content in Media Services by [using customer-managed keys in Azure Key Vault](#).

Migration

For Migration services availability in Azure Government, see [Products available by region](#). For a list of services in scope for DoD IL5 PA, see [Azure Government services by audit scope](#). Guidance below is provided only for IL5 PA services that require extra configuration to support IL5 workloads.

Azure Data Box

- Configure encryption at rest of content in Azure Data Box [using customer-managed keys in Azure Key Vault](#).

Azure Migrate

- Configure encryption at rest of content in Azure Migrate by [using customer-managed keys in Azure Key Vault](#).

Security

For Security services availability in Azure Government, see [Products available by region](#). For a list of services in scope for DoD IL5 PA, see [Azure Government services by audit scope](#). Guidance below is provided only for IL5 PA services that require extra configuration to support IL5 workloads.

Azure Information Protection

- Configure encryption at rest of content in Azure Information Protection [using customer-managed keys in Azure Key Vault](#).

Microsoft Sentinel (formerly Azure Sentinel)

- Configure encryption at rest of content in Microsoft Sentinel by [using customer-managed keys in Azure Key Vault](#).

Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security)

- Configure encryption at rest of content in Microsoft Defender for Cloud Apps [using customer-managed keys in Azure Key Vault](#).

Storage

For Storage services availability in Azure Government, see [Products available by region](#). For a list of services in scope for DoD IL5 PA, see [Azure Government services by audit scope](#). Guidance below is provided only for IL5 PA services that require extra configuration to support IL5 workloads.

Azure Archive Storage

- Azure Archive Storage is a tier of Azure Storage. It automatically helps secure data at rest by using 256-bit AES encryption. Just like hot and cool tiers, Archive Storage can be set at the blob level. To enable access to the content, you need to rehydrate the archived blob or copy it to an online tier, at which point you can enforce customer-managed keys that are in place for your online storage tiers. When you create a target storage account for IL5 data in Archive Storage, add storage encryption via customer-managed keys. For more information, see [Storage encryption with Key Vault managed keys](#).
- The target storage account for Archive Storage can be located in any Azure Government region.

Azure File Sync

- Configure encryption at rest of content in Azure File Sync by [using customer-managed keys in Azure Key Vault](#).

Azure HPC Cache

- Configure encryption at rest of content in Azure HPC Cache [using customer-managed keys in Azure Key Vault](#)

Azure Import/Export

- By default, the Import/Export service will encrypt data that's written to the hard drive for transport. When you create a target storage account for import and export of IL5 data, add storage encryption via customer-managed keys. For more information, see [Storage encryption with Key Vault managed keys](#) in this article.
- The target storage account for import and source storage account for export can be located in any Azure Government region.

Azure NetApp Files

- Configure encryption at rest of content in Azure NetApp Files using customer-managed keys

Azure Storage

Azure Storage consists of multiple data features: Blob storage, File storage, Table storage, and Queue storage. Blob storage supports both standard and premium storage. Premium storage uses only SSDs, to provide the fastest performance possible. Storage also includes configurations that modify these storage types, like hot and cool to provide appropriate speed-of-availability for data scenarios.

Blob storage and File storage always use the account encryption key to encrypt data. Queue storage and Table storage can be [optionally configured](#) to encrypt data with the account encryption key when the storage account is created. You can opt to use customer-managed keys to encrypt data at rest in all Azure Storage features, including Blob, File, Table, and Queue storage. When you use an Azure Storage account, you must follow the steps below to ensure the data is protected with customer-managed keys.

Storage encryption with Key Vault managed keys

To implement Impact Level 5 compliant controls on an Azure Storage account that runs in Azure Government outside of the dedicated DoD regions, you must use encryption at rest with the customer-managed key option enabled. The customer-managed key option is also known as *bring your own key*.

For more information about how to enable this Azure Storage encryption feature, see [Configure encryption with customer-managed keys stored in Azure Key Vault](#).

ⓘ Note

When you use this encryption method, you need to enable it before you add content to the storage account. Any content that's added before the customer-managed key is configured will be protected with Microsoft-managed keys.

StorSimple

- To help ensure the security and integrity of data moved to the cloud, StorSimple allows you to [define cloud storage encryption keys](#). You specify the cloud storage encryption key when you create a volume container.

Next steps

Learn more about Azure Government:

- [Acquiring and accessing Azure Government](#) ↗
- [Azure Government overview](#)
- [Azure Government compliance](#)
- [DoD Impact Level 5](#)
- [DoD in Azure Government](#)
- [Azure Government services by audit scope](#)
- [Azure Government security](#)
- [Azure guidance for secure isolation](#)

Start using Azure Government:

- [Guidance for developers](#)
- [Connect with the Azure Government portal](#)
- [Deploy STIG-compliant Linux VMs](#)
- [Deploy STIG-compliant Windows VMs](#)

Azure guidance for secure isolation

Article • 07/14/2023

Microsoft Azure is a hyperscale public multi-tenant cloud services platform that provides you with access to a feature-rich environment incorporating the latest cloud innovations such as artificial intelligence, machine learning, IoT services, big-data analytics, intelligent edge, and many more to help you increase efficiency and unlock insights into your operations and performance.

A multi-tenant cloud platform implies that multiple customer applications and data are stored on the same physical hardware. Azure uses logical isolation to segregate your applications and data from other customers. This approach provides the scale and economic benefits of multi-tenant cloud services while rigorously helping prevent other customers from accessing your data or applications.

Azure addresses the perceived risk of resource sharing by providing a trustworthy foundation for assuring multi-tenant, cryptographically certain, logically isolated cloud services using a common set of principles:

1. User access controls with authentication and identity separation
2. Compute isolation for processing
3. Networking isolation including data encryption in transit
4. Storage isolation with data encryption at rest
5. Security assurance processes embedded in service design to correctly develop logically isolated services

Multi-tenancy in the public cloud improves efficiency by multiplexing resources among disparate customers at low cost; however, this approach introduces the perceived risk associated with resource sharing. Azure addresses this risk by providing a trustworthy foundation for isolated cloud services using a multi-layered approach depicted in Figure 1.

User access control with authentication and identity separation using Azure Active Directory and Role-Based Access Control (RBAC)

Compute isolation <ul style="list-style-type: none">Logical isolation<ul style="list-style-type: none">HypervisorDrawbridgeUser contextPhysical isolation<ul style="list-style-type: none">Azure Dedicated HostIsolated VMs	Networking isolation <ul style="list-style-type: none">Separation of tenant network trafficData encryption in transitNetwork Security Groups (NSGs)Service TagsAzure Private Link	Storage isolation <ul style="list-style-type: none">Data encryption at rest<ul style="list-style-type: none">Storage service encryptionAzure Disk EncryptionOption for customer managed keys (CMK) in Azure Key Vault
Security assurance processes and practices to correctly develop logically isolated services and systems		

Figure 1. Azure isolation approaches

A brief summary of isolation approaches is provided below.

- User access controls with authentication and identity separation** – All data in Azure irrespective of the type or storage location is associated with a subscription. A cloud tenant can be viewed as a dedicated instance of Microsoft Entra ID that your organization receives and owns when you sign up for a Microsoft cloud service. The identity and access stack helps enforce isolation among subscriptions, including limiting access to resources within a subscription only to authorized users.
- Compute isolation** – Azure provides you with both logical and physical compute isolation for processing. Logical isolation is implemented via:
 - Hypervisor isolation* for services that provide cryptographically certain isolation by using separate virtual machines and using Azure Hypervisor isolation.
 - Drawbridge isolation* inside a virtual machine (VM) for services that provide cryptographically certain isolation for workloads running on the same virtual machine by using isolation provided by [Drawbridge](#). These services provide small units of processing using customer code.
 - User context-based isolation* for services that are composed solely of Microsoft-controlled code and customer code isn't allowed to run.

In addition to robust logical compute isolation available by design to all Azure tenants, if you desire physical compute isolation, you can use Azure Dedicated Host or isolated Virtual Machines, which are deployed on server hardware dedicated to a single customer.

- Networking isolation** – Azure Virtual Network (VNet) helps ensure that your private network traffic is logically isolated from traffic belonging to other

customers. Services can communicate using public IPs or private (VNet) IPs.

Communication between your VMs remains private within a VNet. You can connect your VNets via [VNet peering](#) or [VPN gateways](#), depending on your connectivity options, including bandwidth, latency, and encryption requirements. You can use [network security groups](#) (NSGs) to achieve network isolation and protect your Azure resources from the Internet while accessing Azure services that have public endpoints. You can use Virtual Network [service tags](#) to define network access controls on [network security groups](#) or [Azure Firewall](#). A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, thereby reducing the complexity of frequent updates to network security rules. Moreover, you can use [Private Link](#) to access Azure PaaS services over a private endpoint in your VNet, ensuring that traffic between your VNet and the service travels across the Microsoft global backbone network, which eliminates the need to expose the service to the public Internet. Finally, Azure provides you with options to encrypt data in transit, including [Transport Layer Security \(TLS\)](#) end-to-end encryption of network traffic with [TLS termination using Key Vault certificates](#), [VPN encryption](#) using IPsec, and [Azure ExpressRoute encryption using MACsec with customer-managed keys \(CMK\) support](#).

- **Storage isolation** – To ensure cryptographic certainty of logical data isolation, Azure Storage relies on data encryption at rest using advanced algorithms with multiple ciphers. This process relies on multiple encryption keys and services such as Azure Key Vault and Microsoft Entra ID to ensure secure key access and centralized key management. Azure Storage service encryption ensures that data is automatically encrypted before persisting it to Azure Storage and decrypted before retrieval. All data written to Azure Storage is [encrypted through FIPS 140 validated 256-bit AES encryption](#) and you can use Key Vault for customer-managed keys (CMK). Azure Storage service encryption encrypts the page blobs that store Azure Virtual Machine disks. Moreover, Azure Disk encryption may optionally be used to encrypt Azure Windows and Linux IaaS Virtual Machine disks to increase storage isolation and assure cryptographic certainty of your data stored in Azure. This encryption includes managed disks.
- **Security assurance processes and practices** – Azure isolation assurance is further enforced by Microsoft's internal use of the [Security Development Lifecycle](#) (SDL) and other strong security assurance processes to protect attack surfaces and mitigate threats. Microsoft has established industry-leading processes and tooling that provides high confidence in the Azure isolation guarantee.

In line with the [shared responsibility](#) model in cloud computing, as you migrate workloads from your on-premises datacenter to the cloud, the delineation of responsibility between you and cloud service provider varies depending on the cloud service model. For example, with the Infrastructure as a Service (IaaS) model, Microsoft's responsibility ends at the Hypervisor layer, and you're responsible for all layers above the virtualization layer, including maintaining the base operating system in guest VMs. You can use Azure isolation technologies to achieve the desired level of isolation for your applications and data deployed in the cloud.

Throughout this article, call-out boxes outline important considerations or actions considered to be part of your responsibility. For example, you can use Azure Key Vault to store your secrets, including encryption keys that remain under your control.

Note

Use of Azure Key Vault for customer managed keys (CMK) is optional and represents your responsibility.

Extra resources:

- How to [get started with Key Vault certificates](#)

This article provides technical guidance to address common security and isolation concerns pertinent to cloud adoption. It also explores design principles and technologies available in Azure to help you achieve your secure isolation objectives.

Tip

For recommendations on how to improve the security of applications and data deployed on Azure, you should review the [Azure Security Benchmark](#) documentation.

Identity-based isolation

[Microsoft Entra ID](#) is an identity repository and cloud service that provides authentication, authorization, and access control for your users, groups, and objects. Microsoft Entra ID can be used as a standalone cloud directory or as an integrated solution with existing on-premises Active Directory to enable key enterprise features such as directory synchronization and single sign-on.

Each Azure subscription is associated with a Microsoft Entra tenant. Using [Azure role-based access control \(Azure RBAC\)](#), users, groups, and applications from that directory can be granted access to resources in the Azure subscription. For example, a storage account can be placed in a resource group to control access to that specific storage account using Microsoft Entra ID. Azure Storage defines a set of Azure built-in roles that encompass common permissions used to access blob or queue data. A request to Azure Storage can be authorized using either your Microsoft Entra account or the Storage Account Key. In this manner, only specific users can be given the ability to access data in Azure Storage.

Zero Trust architecture

All data in Azure irrespective of the type or storage location is associated with a subscription. A cloud tenant can be viewed as a dedicated instance of Microsoft Entra ID that your organization receives and owns when you sign up for a Microsoft cloud service. Authentication to the Azure portal is performed through Microsoft Entra ID using an identity created either in Microsoft Entra ID or federated with an on-premises Active Directory. The identity and access stack helps enforce isolation among subscriptions, including limiting access to resources within a subscription only to authorized users. This access restriction is an overarching goal of the [Zero Trust model](#), which assumes that the network is compromised and requires a fundamental shift from the perimeter security model. When evaluating access requests, all requesting users, devices, and applications should be considered untrusted until their integrity can be validated in line with the Zero Trust [design principles](#). Microsoft Entra ID provides the strong, adaptive, standards-based identity verification required in a Zero Trust framework.

Note

Extra resources:

- To learn how to implement Zero Trust architecture on Azure, see [Zero Trust Guidance Center](#).
- For definitions and general deployment models, see [NIST SP 800-207](#) *Zero Trust Architecture*.

Microsoft Entra ID

The separation of the accounts used to administer cloud applications is critical to achieving logical isolation. Account isolation in Azure is achieved using [Microsoft Entra](#)

ID and its capabilities to support granular [Azure role-based access control](#) (Azure RBAC). Each Azure account is associated with one Microsoft Entra tenant. Users, groups, and applications from that directory can manage resources in Azure. You can assign appropriate access rights using the Azure portal, Azure command-line tools, and Azure Management APIs. Each Microsoft Entra tenant is distinct and separate from other Azure ADs. A Microsoft Entra instance is logically isolated using security boundaries to prevent customer data and identity information from comingling, thereby ensuring that users and administrators of one Microsoft Entra ID can't access or compromise data in another Microsoft Entra instance, either maliciously or accidentally. Microsoft Entra ID runs physically isolated on dedicated servers that are logically isolated to a dedicated network segment and where host-level packet filtering and Windows Firewall services provide extra protections from untrusted traffic.

Microsoft Entra ID implements extensive **data protection features**, including tenant isolation and access control, data encryption in transit, secrets encryption and management, disk level encryption, advanced cryptographic algorithms used by various Microsoft Entra components, data operational considerations for insider access, and more. Detailed information is available from a whitepaper [Microsoft Entra Data Security Considerations](#) ↗.

Tenant isolation in Microsoft Entra ID involves two primary elements:

- Preventing data leakage and access across tenants, which means that data belonging to Tenant A can't in any way be obtained by users in Tenant B without explicit authorization by Tenant A.
- Resource access isolation across tenants, which means that operations performed by Tenant A can't in any way impact access to resources for Tenant B.

As shown in Figure 2, access via Microsoft Entra ID requires user authentication through a Security Token Service (STS). The authorization system uses information on the user's existence and enabled state through the Directory Services API and Azure RBAC to determine whether the requested access to the target Microsoft Entra instance is authorized for the user in the session. Aside from token-based authentication that is tied directly to the user, Microsoft Entra ID further supports logical isolation in Azure through:

- Microsoft Entra instances are discrete containers and there's no relationship between them.
- Microsoft Entra data is stored in partitions and each partition has a predetermined set of replicas that are considered the preferred primary replicas. Use of replicas provides high availability of Microsoft Entra services to support identity separation and logical isolation.

- Access isn't permitted across Microsoft Entra instances unless the Microsoft Entra instance administrator grants it through federation or provisioning of user accounts from other Microsoft Entra instances.
- Physical access to servers that comprise the Microsoft Entra service and direct access to Microsoft Entra ID's back-end systems is [restricted to properly authorized Microsoft operational roles](#) using the Just-In-Time (JIT) privileged access management system.
- Microsoft Entra users have no access to physical assets or locations, and therefore it isn't possible for them to bypass the logical Azure RBAC policy checks.

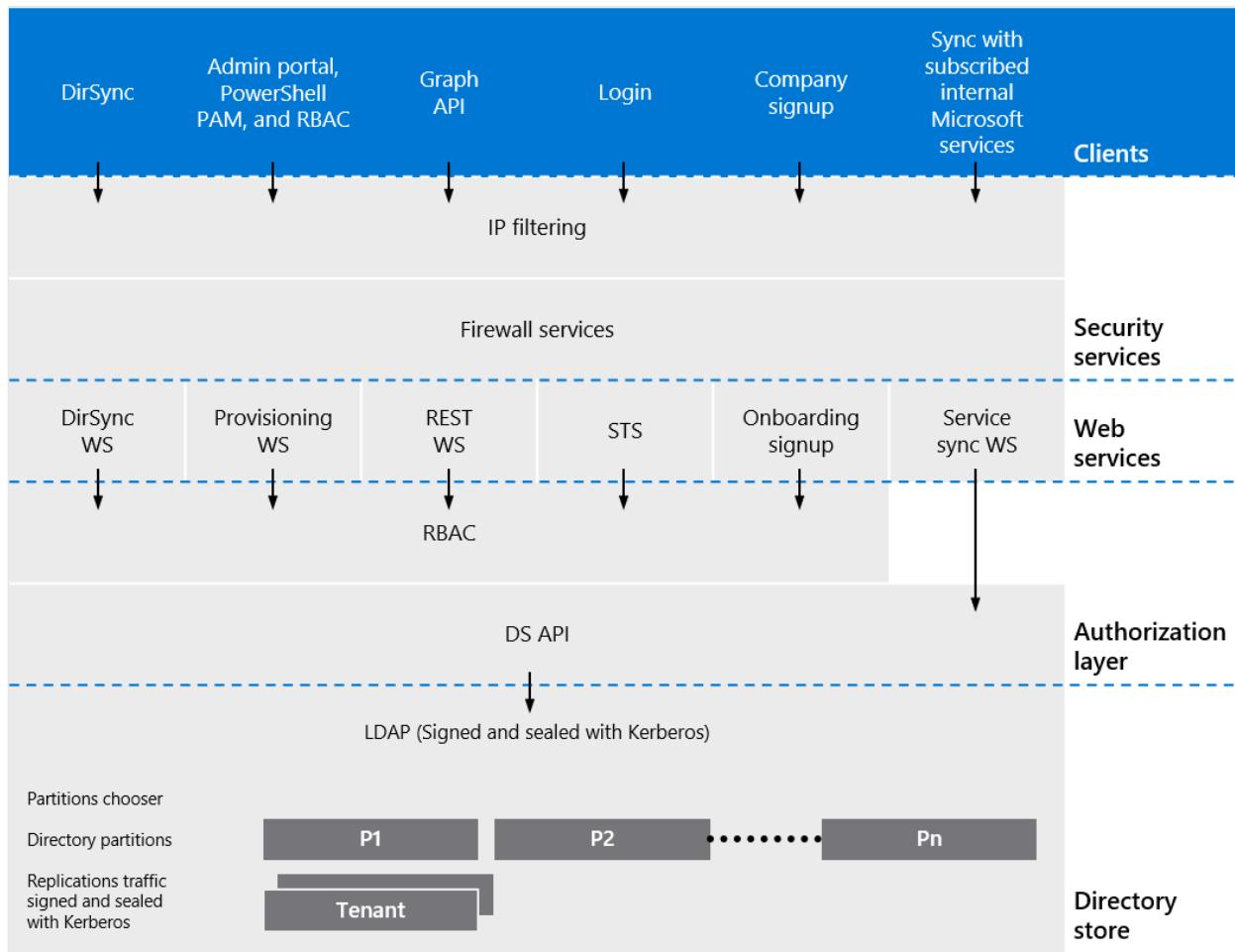


Figure 2. Microsoft Entra logical tenant isolation

In summary, Azure's approach to logical tenant isolation uses identity, managed through Microsoft Entra ID, as the first logical control boundary for providing tenant-level access to resources and authorization through Azure RBAC.

Data encryption key management

Azure has extensive support to safeguard your data using [data encryption](#), including various encryption models:

- Server-side encryption that uses service-managed keys, customer-managed keys in Azure, or customer-managed keys on customer-controlled hardware.
- Client-side encryption that enables you to manage and store keys on premises or in another secure location.

Data encryption provides isolation assurances that are tied directly to encryption (cryptographic) key access. Since Azure uses strong ciphers for data encryption, only entities with access to cryptographic keys can have access to data. Deleting or revoking cryptographic keys renders the corresponding data inaccessible. More information about **data encryption in transit** is provided in [Networking isolation](#) section, whereas **data encryption at rest** is covered in [Storage isolation](#) section.

Azure enables you to enforce **double encryption** for both data at rest and data in transit. With this model, two or more layers of encryption are enabled to protect against compromises of any layer of encryption.

Azure Key Vault

Proper protection and management of cryptographic keys is essential for data security. **Azure Key Vault** is a cloud service for securely storing and managing secrets. The Key Vault service supports two resource types that are described in the rest of this section:

- **Vault** supports software-protected and hardware security module (HSM)-protected secrets, keys, and certificates.
- **Managed HSM** supports only HSM-protected cryptographic keys.

If you require extra security for your most sensitive customer data stored in Azure services, you can encrypt it using your own encryption keys you control in Key Vault.

The Key Vault service provides an abstraction over the underlying HSMs. It provides a REST API to enable service use from cloud applications and authentication through [Microsoft Entra ID](#) to allow you to centralize and customize authentication, disaster recovery, high availability, and elasticity. Key Vault supports [cryptographic keys](#) of various types, sizes, and curves, including RSA and Elliptic Curve keys. With managed HSMs, support is also available for AES symmetric 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, as shown in Figure 3.

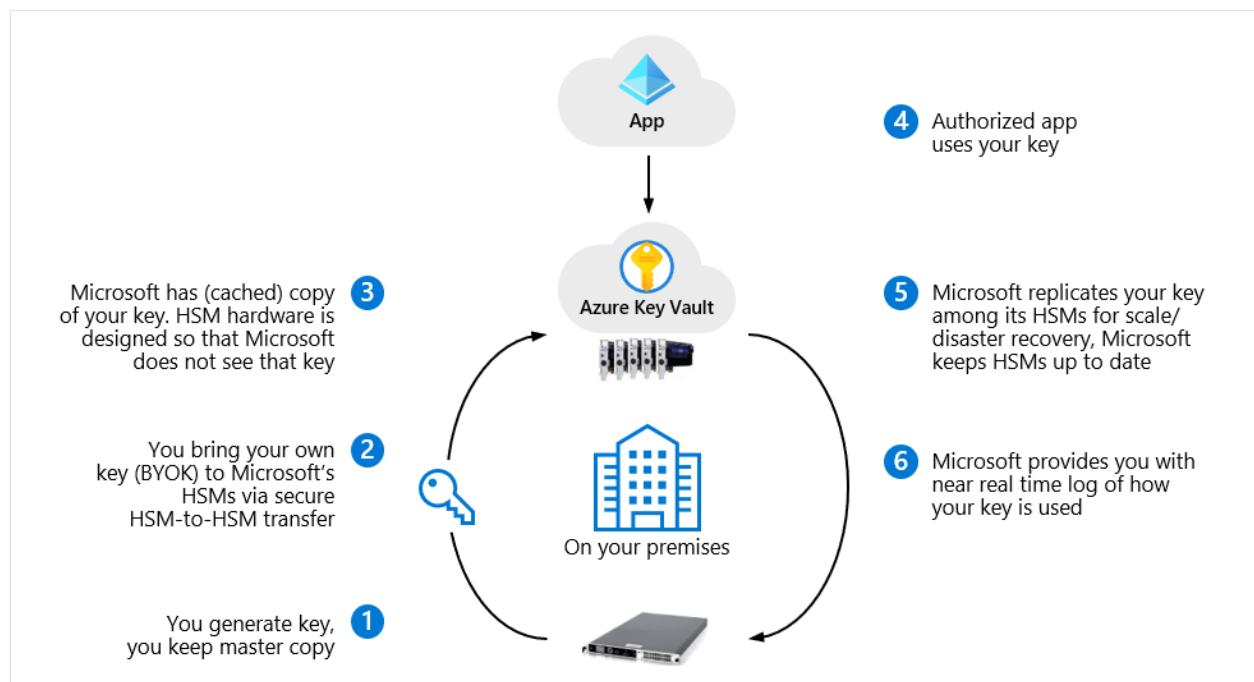


Figure 3. Azure Key Vault support for bring your own key (BYOK)

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. BYOK functionality is available with both [key vaults](#) and [managed HSMs](#). Methods for transferring HSM-protected keys to Key Vault vary depending on the underlying HSM, as explained in online documentation.

ⓘ Note

Azure Key Vault is 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. For more information, see [How does Azure Key Vault protect your keys?](#)

Key Vault provides a robust solution for encryption key lifecycle management. Upon creation, every key vault or managed HSM is automatically associated with the Microsoft Entra tenant that owns the subscription. Anyone trying to manage or retrieve content from a key vault or managed HSM must be properly authenticated and authorized:

- Authentication establishes the identity of the caller (user or application).
- Authorization determines which operations the caller can perform, based on a combination of [Azure role-based access control](#) (Azure RBAC) and key vault access policy or managed HSM local RBAC.

Microsoft Entra ID enforces tenant isolation and implements robust measures to prevent access by unauthorized parties, as described previously in [Microsoft Entra ID](#) section. Access to a key vault or managed HSM is controlled through two interfaces or planes –

management plane and data plane – with both planes using Microsoft Entra ID for authentication.

- **Management plane** enables you to manage the key vault or managed HSM itself, for example, create and delete key vaults or managed HSMs, retrieve key vault or managed HSM properties, and update access policies. For authorization, the management plane uses Azure RBAC with both key vaults and managed HSMs.
- **Data plane** enables you to work with the data stored in your key vaults and managed HSMs, including adding, deleting, and modifying your data. For vaults, stored data can include keys, secrets, and certificates. For managed HSMs, stored data is limited to cryptographic keys only. For authorization, the data plane uses [Key Vault access policy](#) and [Azure RBAC for data plane operations](#) with key vaults, or [managed HSM local RBAC](#) with managed HSMs.

When you create a key vault or managed HSM in an Azure subscription, it's automatically associated with the Microsoft Entra tenant of the subscription. All callers in both planes must register in this tenant and authenticate to access the [key vault](#) or [managed HSM](#).

You control access permissions and can extract detailed activity logs from the Azure Key Vault service. Azure Key Vault logs the following information:

- All authenticated REST API requests, including failed requests
 - Operations on the key vault such as creation, deletion, setting access policies, and so on.
 - Operations on keys and secrets in the key vault, including a) creating, modifying, or deleting keys or secrets, and b) signing, verifying, encrypting keys, and so on.
- Unauthenticated requests such as requests that don't have a bearer token, are malformed or expired, or have an invalid token.

Note

With Azure Key Vault, you can monitor how and when your key vaults and managed HSMs are accessed and by whom.

Extra resources:

- [Configure monitoring and alerting for Azure Key Vault](#)
- [Enable logging for Azure Key Vault](#)
- [How to secure storage account for Azure Key Vault logs](#)

You can also use the [Azure Key Vault solution in Azure Monitor](#) to review Key Vault logs. To use this solution, you need to enable logging of Key Vault diagnostics and direct the diagnostics to a Log Analytics workspace. With this solution, it isn't necessary to write logs to Azure Blob storage.

 **Note**

For a comprehensive list of Azure Key Vault security recommendations, see [Azure security baseline for Key Vault](#).

Vault

Vaults provide a multi-tenant, low-cost, easy to deploy, zone-resilient (where available), and highly available key management solution suitable for most common cloud application scenarios. Vaults can store and safeguard [secrets, keys, and certificates](#). They can be either software-protected (standard tier) or HSM-protected (premium tier). For a comparison between the standard and premium tiers, see the [Azure Key Vault pricing page](#). Software-protected secrets, keys, and certificates are safeguarded by Azure, using industry-standard algorithms and key lengths. If you require extra assurances, you can choose to safeguard your secrets, keys, and certificates in vaults protected by multi-tenant HSMs. The corresponding HSMs are validated according to the [FIPS 140 standard](#), and have an overall Security Level 2 rating, which includes requirements for physical tamper evidence and role-based authentication.

Vaults enable support for [customer-managed keys](#) (CMK) where you can control your own keys in HSMs, and use them to encrypt data at rest for [many Azure services](#). As mentioned previously, you can [import or generate encryption keys](#) in HSMs ensuring that keys never leave the HSM boundary to support *bring your own key (BYOK)* scenarios.

Key Vault can handle requesting and renewing certificates in vaults, including Transport Layer Security (TLS) certificates, enabling you to enroll and automatically renew certificates from supported public Certificate Authorities. Key Vault certificates support provides for the management of your X.509 certificates, which are built on top of keys and provide an automated renewal feature. Certificate owner can [create a certificate](#) through Azure Key Vault or by importing an existing certificate. Both self-signed and Certificate Authority generated certificates are supported. Moreover, the Key Vault certificate owner can implement secure storage and management of X.509 certificates without interaction with private keys.

When you create a key vault in a resource group, you can [manage access](#) by using Microsoft Entra ID, which enables you to grant access at a specific scope level by assigning the appropriate Azure roles. For example, to grant access to a user to manage key vaults, you can assign a predefined key vault Contributor role to the user at a specific scope, including subscription, resource group, or specific resource.

Important

You should control tightly who has Contributor role access to your key vaults. If a user has Contributor permissions to a key vault management plane, the user can gain access to the data plane by setting a key vault access policy.

Extra resources:

- How to [secure access to a key vault](#).

Managed HSM

Managed HSM provides a single-tenant, fully managed, highly available, zone-resilient (where available) HSM as a service to store and manage your cryptographic keys. It's most suitable for applications and usage scenarios that handle high value keys. It also helps you meet the most stringent security, compliance, and regulatory requirements. Managed HSM uses [FIPS 140 Level 3 validated HSMs](#) to protect your cryptographic keys. Each managed HSM pool is an isolated single-tenant instance with its own [security domain](#) controlled by you and isolated cryptographically from instances belonging to other customers. Cryptographic isolation relies on [Intel Software Guard Extensions](#) (SGX) technology that provides encrypted code and data to help ensure your control over cryptographic keys.

When a managed HSM is created, the requestor also provides a list of data plane administrators. Only these administrators are able to [access the managed HSM data plane](#) to perform key operations and manage data plane role assignments (managed HSM local RBAC). The permission model for both the management and data planes uses the same syntax, but permissions are enforced at different levels, and role assignments use different scopes. Management plane Azure RBAC is enforced by Azure Resource Manager while data plane-managed HSM local RBAC is enforced by the managed HSM itself.

Important

Unlike with key vaults, granting your users management plane access to a managed HSM doesn't grant them any access to data plane to access keys or data plane role assignments managed HSM local RBAC. This isolation is implemented by design to prevent inadvertent expansion of privileges affecting access to keys stored in managed HSMs.

As mentioned previously, managed HSM supports [importing keys generated](#) in your on-premises HSMs, ensuring the keys never leave the HSM protection boundary, also known as *bring your own key (BYOK)* scenario. Managed HSM supports integration with Azure services such as [Azure Storage](#), [Azure SQL Database](#), [Azure Information Protection](#), and others. For a more complete list of Azure services that work with Managed HSM, see [Data encryption models](#).

Managed HSM enables you to use the established Azure Key Vault API and management interfaces. You can use the same application development and deployment patterns for all your applications irrespective of the key management solution: multi-tenant vault or single-tenant managed HSM.

Compute isolation

Microsoft Azure compute platform is based on [machine virtualization](#). This approach means that your code – whether it's deployed in a PaaS worker role or an IaaS virtual machine – executes in a virtual machine hosted by a Windows Server Hyper-V hypervisor. On each Azure physical server, also known as a node, there's a [Type 1 Hypervisor](#) that runs directly over the hardware and divides the node into a variable number of Guest virtual machines (VMs), as shown in Figure 4. Each node has one special Host VM, also known as Root VM, which runs the Host OS – a customized and hardened version of the latest Windows Server, which is stripped down to reduce the attack surface and include only those components necessary to manage the node. Isolation of the Root VM from the Guest VMs and the Guest VMs from one another is a key concept in Azure security architecture that forms the basis of Azure [compute isolation](#), as described in Microsoft online documentation.

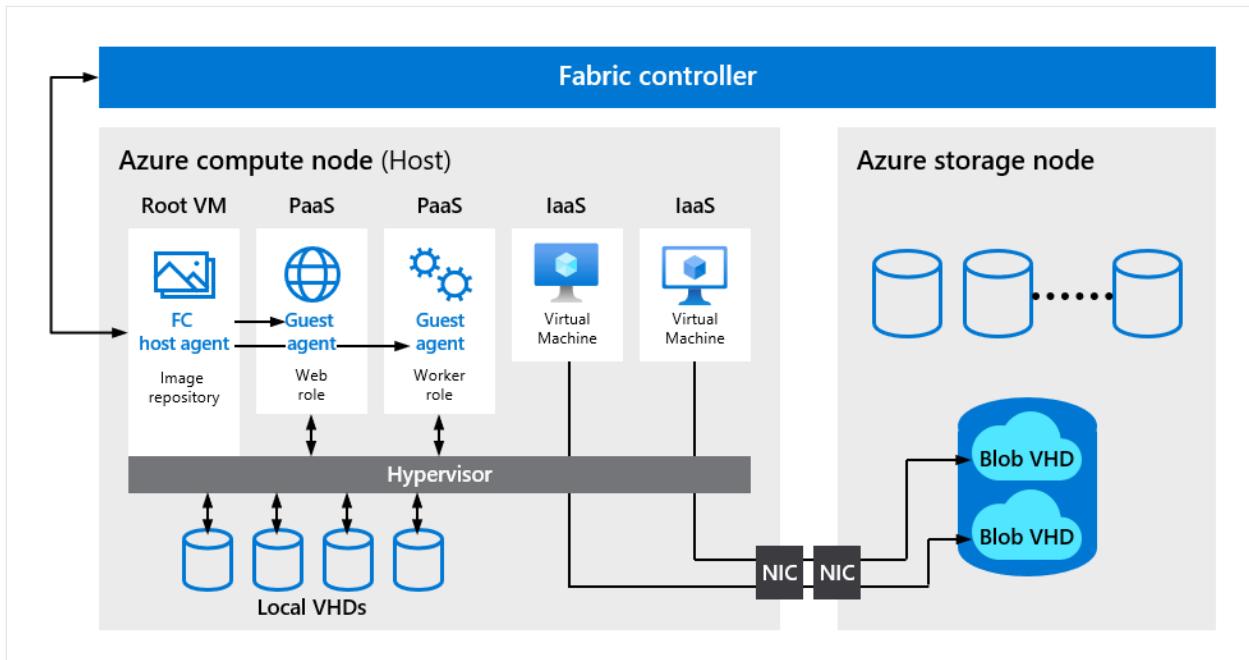


Figure 4. Isolation of Hypervisor, Root VM, and Guest VMs

Physical servers hosting VMs are grouped into clusters, and they're independently managed by a scaled-out and redundant platform software component called the **Fabric Controller** (FC). Each FC manages the lifecycle of VMs running in its cluster, including provisioning and monitoring the health of the hardware under its control. For example, the FC is responsible for recreating VM instances on healthy servers when it determines that a server has failed. It also allocates infrastructure resources to tenant workloads, and it manages unidirectional communication from the Host to virtual machines. Dividing the compute infrastructure into clusters, isolates faults at the FC level and prevents certain classes of errors from affecting servers beyond the cluster in which they occur.

The FC is the brain of the Azure compute platform and the Host Agent is its proxy, integrating servers into the platform so that the FC can deploy, monitor, and manage the virtual machines used by you and Azure cloud services. The Hypervisor/Host OS pairing uses decades of Microsoft's experience in operating system security, including security focused investments in [Microsoft Hyper-V](#) to provide strong isolation of Guest VMs. Hypervisor isolation is discussed later in this section, including assurances for strongly defined security boundaries enforced by the Hypervisor, defense-in-depth exploits mitigations, and strong security assurance processes.

Management network isolation

There are three Virtual Local Area Networks (VLANs) in each compute hardware cluster, as shown in Figure 5:

- Main VLAN interconnects untrusted customer nodes,

- Fabric Controller (FC) VLAN that contains trusted FCs and supporting systems, and
- Device VLAN that contains trusted network and other infrastructure devices.

Communication is permitted from the FC VLAN to the main VLAN but can't be initiated from the main VLAN to the FC VLAN. The bridge from the FC VLAN to the Main VLAN is used to reduce the overall complexity and improve reliability/resiliency of the network. The connection is secured in several ways to ensure that commands are trusted and successfully routed:

- Communication from an FC to a Fabric Agent (FA) is unidirectional and requires mutual authentication via certificates. The FA implements a TLS-protected service that only responds to requests from the FC. It can't initiate connections to the FC or other privileged internal nodes.
- The FC treats responses from the agent service as if they were untrusted. Communication with the agent is further restricted to a set of authorized IP addresses using firewall rules on each physical node, and routing rules at the border gateways.
- Throttling is used to ensure that customer VMs can't saturate the network and management commands from being routed.

Communication is also blocked from the main VLAN to the device VLAN. This way, even if a node running customer code is compromised, it can't attack nodes on either the FC or device VLANs.

These controls ensure that management console's access to the Hypervisor is always valid and available.

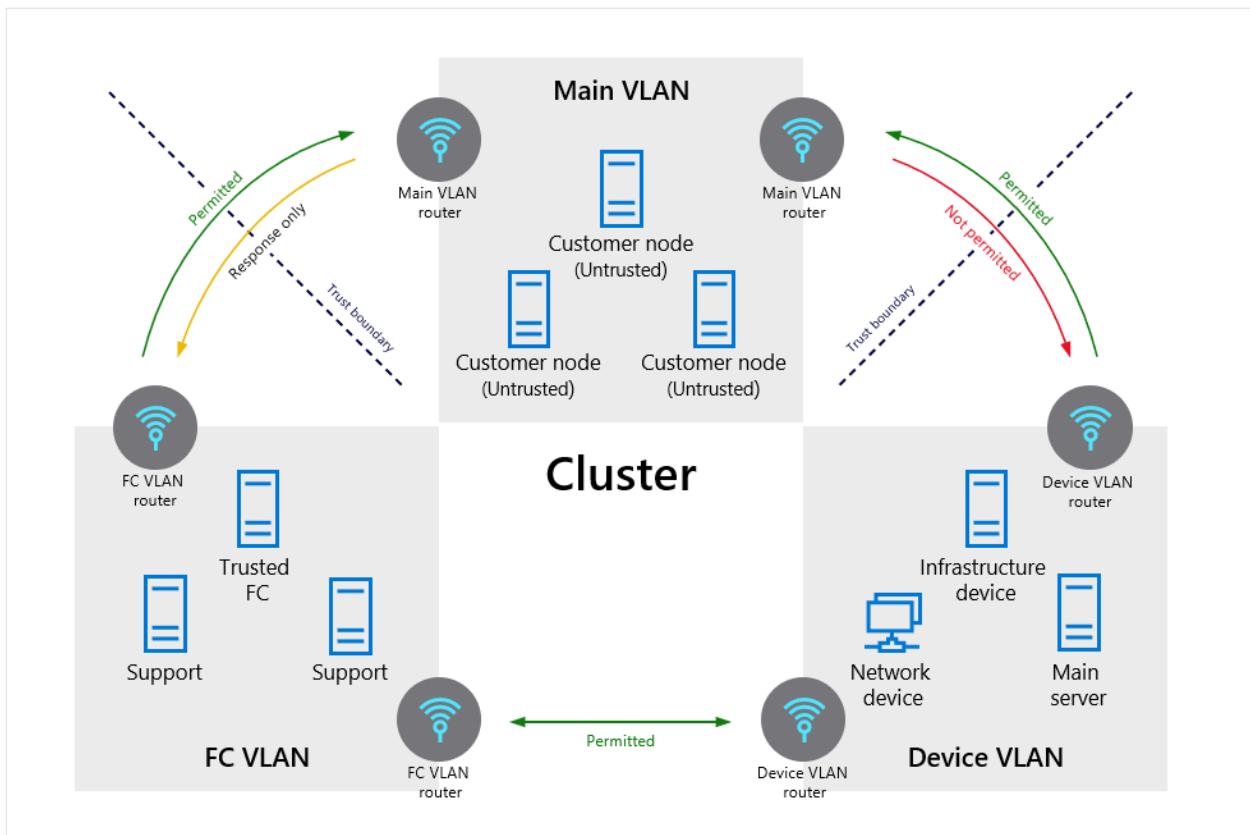


Figure 5. VLAN isolation

The Hypervisor and the Host OS provide network packet filters, which help ensure that untrusted VMs can't generate spoofed traffic or receive traffic not addressed to them, direct traffic to protected infrastructure endpoints, or send/receive inappropriate broadcast traffic. By default, traffic is blocked when a VM is created, and then the FC agent configures the packet filter to add rules and exceptions to allow authorized traffic. More detailed information about network traffic isolation and separation of tenant traffic is provided in [Networking isolation](#) section.

Management console and management plane

The Azure Management Console and Management Plane follow strict security architecture principles of least privilege to secure and isolate tenant processing:

- **Management Console (MC)** – The MC in Azure Cloud is composed of the Azure portal GUI and the Azure Resource Manager API layers. They both use user credentials to authenticate and authorize all operations.
- **Management Plane (MP)** – This layer performs the actual management actions and is composed of the Compute Resource Provider (CRP), Fabric Controller (FC), Fabric Agent (FA), and the underlying Hypervisor, which has its own Hypervisor Agent to service communication. These layers all use system contexts that are granted the least permissions needed to perform their operations.

The Azure FC allocates infrastructure resources to tenants and manages unidirectional communications from the Host OS to Guest VMs. The VM placement algorithm of the Azure FC is highly sophisticated and nearly impossible to predict. The FA resides in the Host OS and it manages tenant VMs. The collection of the Azure Hypervisor, Host OS and FA, and customer VMs constitute a compute node, as shown in Figure 4. FCs manage FAs although FCs exist outside of compute nodes – separate FCs exist to manage compute and storage clusters. If you update your application's configuration file while running in the MC, the MC communicates through CRP with the FC, and the FC communicates with the FA.

CRP is the front-end service for Azure Compute, exposing consistent compute APIs through Azure Resource Manager, thereby enabling you to create and manage virtual machine resources and extensions via simple templates.

Communications among various components (for example, Azure Resource Manager to and from CRP, CRP to and from FC, FC to and from Hypervisor Agent) all operate on different communication channels with different identities and different permissions sets. This design follows common least-privilege models to ensure that a compromise of any single layer will prevent more actions. Separate communications channels ensure that communications can't bypass any layer in the chain. Figure 6 illustrates how the MC and MP securely communicate within the Azure cloud for Hypervisor interaction initiated by a user's [OAuth 2.0 authentication to Microsoft Entra ID](#).

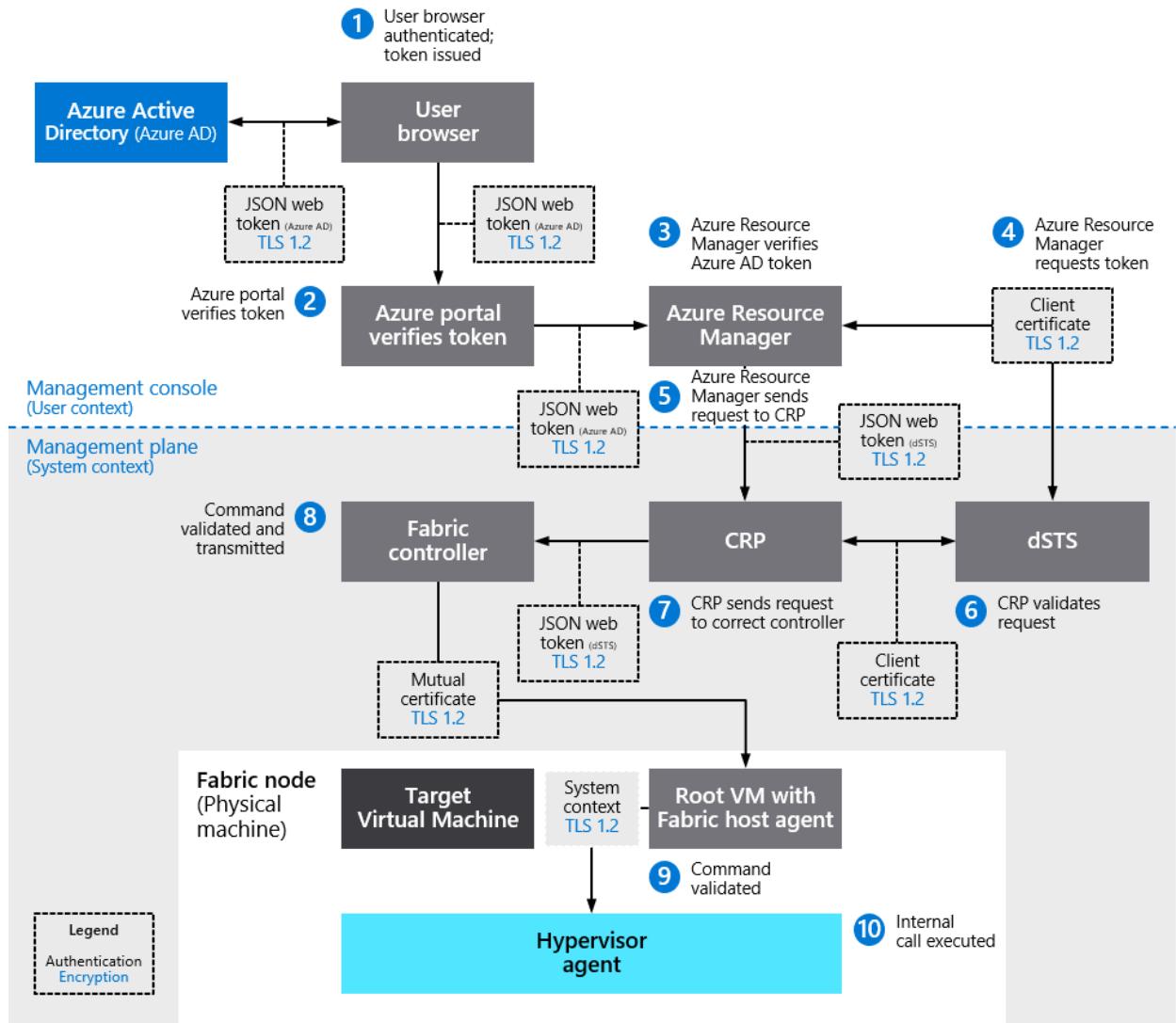


Figure 6. Management Console and Management Plane interaction for secure management flow

All management commands are authenticated via RSA signed certificate or JSON Web Token (JWT). Authentication and command channels are encrypted via Transport Layer Security (TLS) 1.2 as described in [Data encryption in transit](#) section. Server certificates are used to provide TLS connectivity to the authentication providers where a separate authorization mechanism is used, for example, Microsoft Entra ID or datacenter Security Token Service (dSTS). dSTS is a token provider like Microsoft Entra ID that is isolated to the Microsoft datacenter and used for service level communications.

Figure 6 illustrates the management flow corresponding to a user command to stop a virtual machine. The steps enumerated in Table 1 apply to other management commands in the same way and use the same encryption and authentication flow.

Table 1. Management flow involving various MC and MP components

Expand table

Step	Description	Authentication	Encryption
1.	User authenticates via Microsoft Entra ID by providing credentials and is issued a token.	User Credentials	TLS 1.2
2.	Browser presents token to Azure portal to authenticate user. Azure portal verifies token using token signature and valid signing keys.	JSON Web Token (Microsoft Entra ID)	TLS 1.2
3.	User issues "stop VM" request on Azure portal. Azure portal sends "stop VM" request to Azure Resource Manager and presents user's token that was provided by Microsoft Entra ID. Azure Resource Manager verifies token using token signature and valid signing keys and that the user is authorized to perform the requested operation.	JSON Web Token (Microsoft Entra ID)	TLS 1.2
4.	Azure Resource Manager requests a token from dSTS server based on the client certificate that Azure Resource Manager has, enabling dSTS to grant a JSON Web Token with the correct identity and roles.	Client Certificate	TLS 1.2
5.	Azure Resource Manager sends request to CRP. Call is authenticated via OAuth using a JSON Web Token representing the Azure Resource Manager system identity from dSTS, thus transition from user to system context.	JSON Web Token (dSTS)	TLS 1.2
6.	CRP validates the request and determines which fabric controller can complete the request. CRP requests a certificate from dSTS based on its client certificate so that it can connect to the specific Fabric Controller (FC) that is the target of the command. Token will grant permissions only to that specific FC if CRP is allowed to communicate to that FC.	Client Certificate	TLS 1.2
7.	CRP then sends the request to the correct FC with the JSON Web Token that was created by dSTS.	JSON Web Token (dSTS)	TLS 1.2
8.	FC then validates the command is allowed and comes from a trusted source. Then it establishes a secure TLS connection to the correct Fabric Agent (FA) in the cluster that can execute the command by using a certificate that is unique to the target FA and the FC. Once the secure connection is established, the command is transmitted.	Mutual Certificate	TLS 1.2
9.	The FA again validates the command is allowed and comes from a trusted source. Once validated, the FA will establish a secure connection using mutual	Mutual Certificate	TLS 1.2

Step	Description	Authentication	Encryption
	certificate authentication and issue the command to the Hypervisor Agent that is only accessible by the FA.		
10.	Hypervisor Agent on the host executes an internal call to stop the VM.	System Context	N.A.

Commands generated through all steps of the process identified in this section and sent to the FC and FA on each node, are written to a local audit log, and distributed to multiple analytics systems for stream processing in order to monitor system health and track security events and patterns. Tracking includes events that were processed successfully and events that were invalid. Invalid requests are processed by the intrusion detection systems to detect anomalies.

Logical isolation implementation options

Azure provides isolation of compute processing through a multi-layered approach, including:

- **Hypervisor isolation** for services that provide cryptographically certain isolation by using separate virtual machines and using Azure Hypervisor isolation. Examples: *App Service, Azure Container Instances, Azure Databricks, Azure Functions, Azure Kubernetes Service, Azure Machine Learning, Cloud Services, Data Factory, Service Fabric, Virtual Machines, Virtual Machine Scale Sets*.
- **Drawbridge isolation** inside a VM for services that provide cryptographically certain isolation to workloads running on the same virtual machine by using isolation provided by [Drawbridge](#). These services provide small units of processing using customer code. To provide security isolation, Drawbridge runs a user process together with a light-weight version of the Windows kernel (library OS) inside a *pico-process*. A pico-process is a secured process with no direct access to services or resources of the Host system. Examples: *Automation, Azure Database for MySQL, Azure Database for PostgreSQL, Azure SQL Database, Azure Stream Analytics*.
- **User context-based isolation** for services that are composed solely of Microsoft-controlled code and customer code isn't allowed to run. Examples: *API Management, Application Gateway, Microsoft Entra ID, Azure Backup, Azure Cache for Redis, Azure DNS, Azure Information Protection, Azure IoT Hub, Azure Key Vault, Azure portal, Azure Monitor (including Log Analytics), Microsoft Defender for Cloud, Azure Site Recovery, Container Registry, Content Delivery Network, Event Grid, Event Hubs, Load Balancer, Service Bus, Storage, Virtual Network, VPN Gateway, Traffic Manager*.

These logical isolation options are discussed in the rest of this section.

Hypervisor isolation

Hypervisor isolation in Azure is based on [Microsoft Hyper-V](#) technology, which enables Azure Hypervisor-based isolation to benefit from decades of Microsoft experience in operating system security and investments in Hyper-V technology for virtual machine isolation. You can review independent third-party assessment reports about Hyper-V security functions, including the [National Information Assurance Partnership \(NIAP\) Common Criteria Evaluation and Validation Scheme \(CCEVS\) reports](#) such as the [report published in Feb-2021](#) that is discussed herein.

The Target of Evaluation (TOE) was composed of Microsoft Windows Server, Microsoft Windows 10 version 1909 (November 2019 Update), and Microsoft Windows Server 2019 (version 1809) Hyper-V ("Windows"). TOE enforces the following security policies as described in the report:

- **Security Audit** – Windows has the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs. Audit information generated by the system includes the date and time of the event, the user identity that caused the event to be generated, and other event-specific data. Authorized administrators can review, search, and sort audit records. Authorized administrators can also configure the audit system to include or exclude potentially auditable events to be audited based on many characteristics. In the context of this evaluation, the protection profile requirements cover generating audit events, authorized review of stored audit records, and providing secure storage for audit event entries.
- **Cryptographic Support** – Windows provides validated cryptographic functions that support encryption/decryption, cryptographic signatures, cryptographic hashing, and random number generation. Windows implements these functions in support of IPsec, TLS, and HTTPS protocol implementation. Windows also ensures that its Guest VMs have access to entropy data so that virtualized operating systems can ensure the implementation of strong cryptography.
- **User Data Protection** – Windows makes certain computing services available to Guest VMs but implements measures to ensure that access to these services is granted on an appropriate basis and that these interfaces don't result in unauthorized data leakage between Guest VMs and Windows or between multiple Guest VMs.
- **Identification and Authentication** – Windows offers several methods of user authentication, which includes X.509 certificates needed for trusted protocols. Windows implements password strength mechanisms and ensures that excessive

failed authentication attempts using methods subject to brute force guessing (password, PIN) results in lockout behavior.

- **Security Management** – Windows includes several functions to manage security policies. Access to administrative functions is enforced through administrative roles. Windows also has the ability to support the separation of management and operational networks and to prohibit data sharing between Guest VMs.
- **Protection of the TOE Security Functions (TSF)** – Windows implements various self-protection mechanisms to ensure that it can't be used as a platform to gain unauthorized access to data stored on a Guest VM, that the integrity of both the TSF and its Guest VMs is maintained, and that Guest VMs are accessed solely through well-documented interfaces.
- **TOE Access** – In the context of this evaluation, Windows allows an authorized administrator to configure the system to display a logon banner before the logon dialog.
- **Trusted Path/Channels** – Windows implements IPsec, TLS, and HTTPS trusted channels and paths for remote administration, transfer of audit data to the operational environment, and separation of management and operational networks.

More information is available from the [third-party certification report](#) .

The critical Hypervisor isolation is provided through:

- Strongly defined security boundaries enforced by the Hypervisor
- Defense-in-depth exploits mitigations
- Strong security assurance processes

These technologies are described in the rest of this section. **They enable Azure Hypervisor to offer strong security assurances for tenant separation in a multi-tenant cloud.**

Strongly defined security boundaries

Your code executes in a Hypervisor VM and benefits from Hypervisor enforced security boundaries, as shown in Figure 7. Azure Hypervisor is based on [Microsoft Hyper-V](#) technology. It divides an Azure node into a variable number of Guest VMs that have separate address spaces where they can load an operating system (OS) and applications operating in parallel to the Host OS that executes in the Root partition of the node.

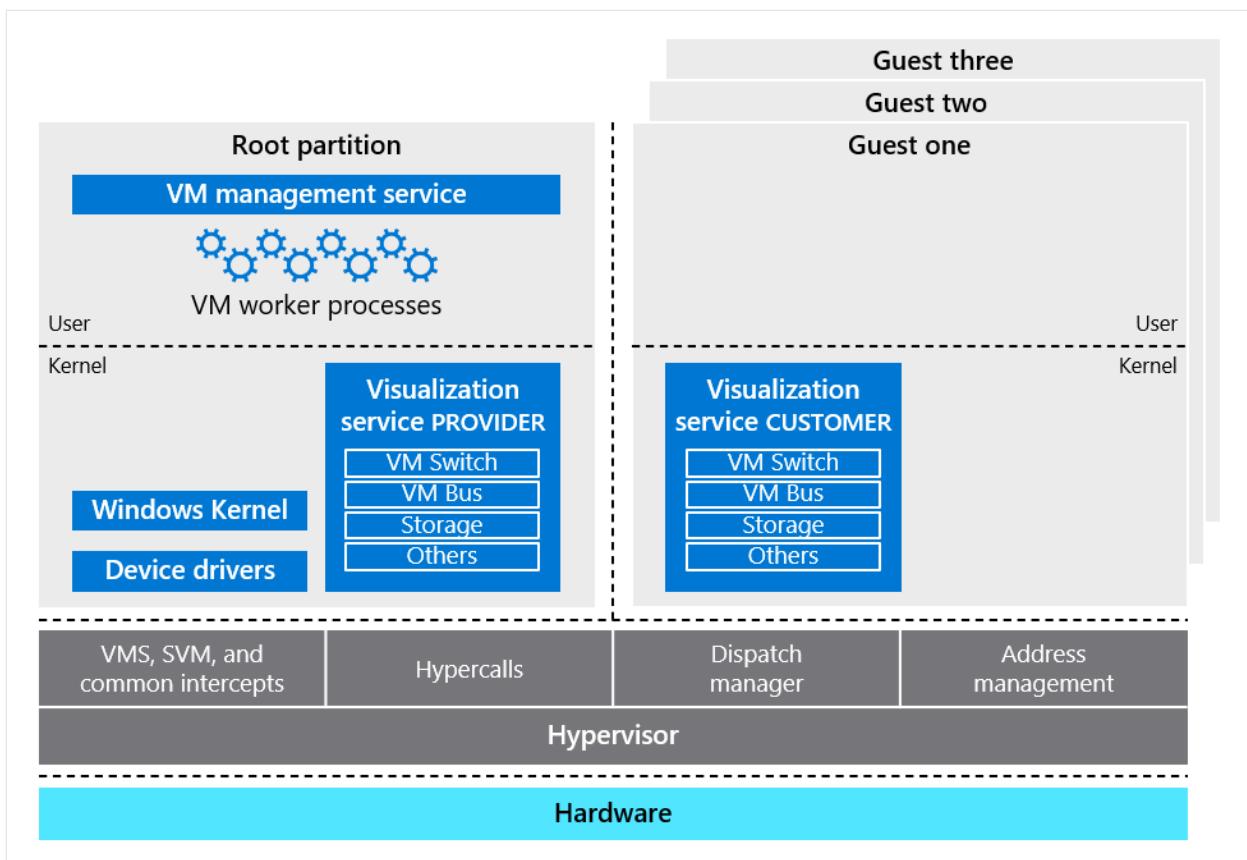


Figure 7. Compute isolation with Azure Hypervisor (see online [glossary of terms](#))

The Azure Hypervisor acts like a micro-kernel, passing all hardware access requests from Guest VMs using a Virtualization Service Client (VSC) to the Host OS for processing by using a shared-memory interface called VMBus. The Host OS proxies the hardware requests using a Virtualization Service Provider (VSP) that prevents users from obtaining raw read/write/execute access to the system and mitigates the risk of sharing system resources. The privileged Root partition, also known as Host OS, has direct access to the physical devices/peripherals on the system, for example, storage controllers, GPUs, networking adapters, and so on. The Host OS allows Guest partitions to share the use of these physical devices by exposing virtual devices to each Guest partition. So, an operating system executing in a Guest partition has access to virtualized peripheral devices that are provided by VSPs executing in the Root partition. These virtual device representations can take one of three forms:

- **Emulated devices** – The Host OS may expose a virtual device with an interface identical to what would be provided by a corresponding physical device. In this case, an operating system in a Guest partition would use the same device drivers as it does when running on a physical system. The Host OS would emulate the behavior of a physical device to the Guest partition.
- **Para-virtualized devices** – The Host OS may expose virtual devices with a virtualization-specific interface using the VMBus shared memory interface between the Host OS and the Guest. In this model, the Guest partition uses device drivers

specifically designed to implement a virtualized interface. These para-virtualized devices are sometimes referred to as “synthetic” devices.

- **Hardware-accelerated devices** – The Host OS may expose actual hardware peripherals directly to the Guest partition. This model allows for high I/O performance in a Guest partition, as the Guest partition can directly access hardware device resources without going through the Host OS. [Azure Accelerated Networking](#) is an example of a hardware accelerated device. Isolation in this model is achieved using input-output memory management units (I/O MMUs) to provide address space and interrupt isolation for each partition.

Virtualization extensions in the Host CPU enable the Azure Hypervisor to enforce isolation between partitions. The following fundamental CPU capabilities provide the hardware building blocks for Hypervisor isolation:

- **Second-level address translation** – the Hypervisor controls what memory resources a partition is allowed to access by using second-level page tables provided by the CPU’s memory management unit (MMU). The CPU’s MMU uses second-level address translation under Hypervisor control to enforce protection on memory accesses performed by:
 - CPU when running under the context of a partition.
 - I/O devices that are being accessed directly by Guest partitions.
- **CPU context** – the Hypervisor uses virtualization extensions in the CPU to restrict privileges and CPU context that can be accessed while a Guest partition is running. The Hypervisor also uses these facilities to save and restore state when sharing CPUs between multiple partitions to ensure isolation of CPU state between the partitions.

The Azure Hypervisor makes extensive use of these processor facilities to provide isolation between partitions. The emergence of speculative side channel attacks has identified potential weaknesses in some of these processor isolation capabilities. In a multi-tenant architecture, any cross-VM attack across different tenants involves two steps: placing an adversary-controlled VM on the same Host as one of the victim VMs, and then breaching the logical isolation boundary to perform a side-channel attack.

Azure provides protection from both threat vectors by using an advanced VM placement algorithm enforcing memory and process separation for logical isolation, and secure network traffic routing with cryptographic certainty at the Hypervisor. As discussed in section titled [Exploitation of vulnerabilities in virtualization technologies](#) later in the article, the Azure Hypervisor has been architected to provide robust isolation directly within the hypervisor that helps mitigate many sophisticated side channel attacks.

The Azure Hypervisor defined security boundaries provide the base level isolation primitives for strong segmentation of code, data, and resources between potentially hostile multi-tenants on shared hardware. These isolation primitives are used to create multi-tenant resource isolation scenarios including:

- **Isolation of network traffic between potentially hostile guests** – Virtual Network (VNet) provides isolation of network traffic between tenants as part of its fundamental design, as described later in *Separation of tenant network traffic* section. VNet forms an isolation boundary where the VMs within a VNet can only communicate with each other. Any traffic destined to a VM from within the VNet or external senders without the proper policy configured will be dropped by the Host and not delivered to the VM.
- **Isolation for encryption keys and cryptographic material** – You can further augment the isolation capabilities with the use of [hardware security managers](#) or [specialized key storage](#), for example, storing encryption keys in FIPS 140 validated hardware security modules (HSMs) via [Azure Key Vault](#).
- **Scheduling of system resources** – Azure design includes guaranteed availability and segmentation of compute, memory, storage, and both direct and para-virtualized device access.

The Azure Hypervisor meets the security objectives shown in Table 2.

Table 2. Azure Hypervisor security objectives

Expand table

Objective	Source
Isolation	The Azure Hypervisor security policy mandates no information transfer between VMs. This policy requires capabilities in the Virtual Machine Manager (VMM) and hardware for the isolation of memory, devices, networking, and managed resources such as persisted data.
VMM integrity	Integrity is a core security objective for virtualization systems. To achieve system integrity, the integrity of each Hypervisor component is established and maintained. This objective concerns only the integrity of the Hypervisor itself, not the integrity of the physical platform or software running inside VMs.
Platform integrity	The integrity of the Hypervisor depends on the integrity of the hardware and software on which it relies. Although the Hypervisor doesn't have direct control over the integrity of the platform, Azure relies on hardware and firmware mechanisms such as the Cerberus security microcontroller to protect the underlying platform integrity , thereby preventing the VMM and Guests from running should platform integrity be compromised.

Objective	Source
Management access	Management functions are exercised only by authorized administrators, connected over secure connections with a principle of least privilege enforced by fine grained role access control mechanism.
Audit	Azure provides audit capability to capture and protect system data so that it can later be inspected.

Defense-in-depth exploits mitigations

To further mitigate the risk of a security compromise, Microsoft has invested in numerous defense-in-depth mitigations in Azure systems software, hardware, and firmware to provide strong real-world isolation guarantees to Azure customers. As mentioned previously, Azure Hypervisor isolation is based on [Microsoft Hyper-V](#) technology, which enables Azure Hypervisor to benefit from decades of Microsoft experience in operating system security and investments in Hyper-V technology for virtual machine isolation.

Listed below are some key design principles adopted by Microsoft to secure Hyper-V:

- Prevent design level issues from affecting the product
 - Every change going into Hyper-V is subject to design review.
- Eliminate common vulnerability classes with safer coding
 - Some components such as the VMSSwitch use a formally proven protocol parser.
 - Many components use `gs1::span` instead of raw pointers, which eliminates the possibility of buffer overflows and/or out-of-bounds memory accesses. For more information, see the [Guidelines Support Library \(GSL\)](#) documentation.
 - Many components use [smart pointers](#) to eliminate the risk of [use-after-free](#) bugs.
 - Most Hyper-V kernel-mode code uses a heap allocator that zeros on allocation to eliminate uninitialized memory bugs.
- Eliminate common vulnerability classes with compiler mitigations
 - All Hyper-V code is compiled with InitAll, which [eliminates uninitialized stack variables](#). This approach was implemented because many historical vulnerabilities in Hyper-V were caused by uninitialized stack variables.
 - All Hyper-V code is compiled with [stack canaries](#) to dramatically reduce the risk of stack overflow vulnerabilities.
- Find issues that make their way into the product
 - All Windows code has a set of static analysis rules run across it.
 - All Hyper-V code is code reviewed and fuzzed. For more information on fuzzing, see [Security assurance processes and practices](#) section later in this article.

- Make exploitation of remaining vulnerabilities more difficult
 - The VM worker process has the following mitigations applied:
 - [Arbitrary Code Guard](#) – Dynamically generated code can't be loaded in the VM Worker process.
 - [Code Integrity Guard](#) – Only Microsoft signed code can be loaded in the VM Worker Process.
 - [Control Flow Guard \(CFG\)](#) – Provides course grained control flow protection to indirect calls and jumps.
 - NoChildProcess – The worker process can't create child processes (useful for bypassing CFG).
 - NoLowImages / NoRemoteImages – The worker process can't load DLLs over the network or DLLs that were written to disk by a sandboxed process.
 - NoWin32k – The worker process can't communicate with Win32k, which makes sandbox escapes more difficult.
 - Heap randomization – Windows ships with one of the most secure heap implementations of any operating system.
 - [Address Space Layout Randomization \(ASLR\)](#) – Randomizes the layout of heaps, stacks, binaries, and other data structures in the address space to make exploitation less reliable.
 - [Data Execution Prevention \(DEP/NX\)](#) – Only pages of memory intended to contain code are executable.
 - The kernel has the following mitigations applied:
 - Heap randomization – Windows ships with one of the most secure heap implementations of any operating system.
 - [Address Space Layout Randomization \(ASLR\)](#) – Randomizes the layout of heaps, stacks, binaries, and other data structures in the address space to make exploitation less reliable.
 - [Data Execution Prevention \(DEP/NX\)](#) – Only pages of memory intended to contain code are executable.

Microsoft investments in Hyper-V security benefit Azure Hypervisor directly. The goal of defense-in-depth mitigations is to make weaponized exploitation of a vulnerability as expensive as possible for an attacker, limiting their impact and maximizing the window for detection. All exploit mitigations are evaluated for effectiveness by a thorough security review of the Azure Hypervisor attack surface using methods that adversaries may employ. Table 3 outlines some of the mitigations intended to protect the Hypervisor isolation boundaries and hardware host integrity.

Table 3. Azure Hypervisor defense-in-depth

Mitigation	Security Impact	Mitigation Details
Control flow integrity	Increases cost to perform control flow integrity attacks (for example, return oriented programming exploits)	Control Flow Guard (CFG) ensures indirect control flow transfers are instrumented at compile time and enforced by the kernel (user-mode) or secure kernel (kernel-mode), mitigating stack return vulnerabilities.
User-mode code integrity	Protects against malicious and unwanted binary execution in user mode	Address Space Layout Randomization (ASLR) forced on all binaries in host partition, all code compiled with SDL security checks (for example, <code>strict_gs</code>), arbitrary code generation restrictions in place on host processes prevent injection of runtime-generated code.
Hypervisor enforced user and kernel mode code integrity	No code loaded into code pages marked for execution until authenticity of code is verified	Virtualization-based Security (VBS) uses memory isolation to create a secure world to enforce policy and store sensitive code and secrets. With Hypervisor enforced Code Integrity (HVCI), the secure world is used to prevent unsigned code from being injected into the normal world kernel.
Hardware root-of-trust with platform secure boot	Ensures host only boots exact firmware and OS image required	Windows secure boot validates that Azure Hypervisor infrastructure is only bootable in a known good configuration, aligned to Azure firmware, hardware, and kernel production versions.
Reduced attack surface VMM	Protects against escalation of privileges in VMM user functions	The Azure Hypervisor Virtual Machine Manager (VMM) contains both user and kernel mode components. User mode components are isolated to prevent break-out into kernel mode functions in addition to numerous layered mitigations.

Moreover, Azure has adopted an assume-breach security strategy implemented via [Red Teaming](#). This approach relies on a dedicated team of security researchers and engineers who conduct continuous ongoing testing of Azure systems and operations using the same tactics, techniques, and procedures as real adversaries against live production infrastructure, without the foreknowledge of the Azure infrastructure and platform engineering or operations teams. This approach tests security detection and response capabilities and helps identify production vulnerabilities in Azure Hypervisor and other systems, including configuration errors, invalid assumptions, or other security issues in a controlled manner. Microsoft invests heavily in these innovative security measures for continuous Azure threat mitigation.

Strong security assurance processes

The attack surface in Hyper-V is [well understood](#) and has been the subject of [ongoing research](#) and thorough security reviews. Microsoft has been transparent about the Hyper-V attack surface and underlying security architecture as demonstrated during a public [presentation at a Black Hat conference](#) in 2018. Microsoft stands behind the robustness and quality of Hyper-V isolation with a [\\$250,000 bug bounty program](#) for critical Remote Code Execution (RCE), information disclosure, and Denial of Service (DOS) vulnerabilities reported in Hyper-V. By using the same Hyper-V technology in Windows Server and Azure cloud platform, the publicly available documentation and bug bounty program ensure that security improvements will accrue to all users of Microsoft products and services. Table 4 summarizes the key attack surface points from the Black Hat presentation.

Table 4. Hyper-V attack surface details

[Expand table](#)

Attack surface area	Privileges granted if compromised	High-level components
Hyper-V	Hypervisor: full system compromise with the ability to compromise other Guests	- Hypercalls - Intercept handling
Host partition kernel-mode components	System in kernel mode: full system compromise with the ability to compromise other Guests	- Virtual Infrastructure Driver (VID) intercept handling - Kernel-mode client library - Virtual Machine Bus (VMBus) channel messages - Storage Virtualization Service Provider (VSP) - Network VSP - Virtual Hard Disk (VHD) parser - Azure Networking Virtual Filtering Platform (VFP) and Virtual Network (VNet)
Host partition user-mode components	Worker process in user mode: limited compromise with ability to attack Host and elevate privileges	- Virtual devices (VDEVs)

To protect these attack surfaces, Microsoft has established industry-leading processes and tooling that provide high confidence in the Azure isolation guarantee. As described in [Security assurance processes and practices](#) section later in this article, the approach includes purpose-built fuzzing, penetration testing, security development lifecycle, mandatory security training, security reviews, security intrusion detection based on Guest – Host threat indicators, and automated build alerting of changes to the attack

surface area. This mature multi-dimensional assurance process helps augment the isolation guarantees provided by the Azure Hypervisor by mitigating the risk of security vulnerabilities.

ⓘ Note

Azure has adopted an industry leading approach to ensure Hypervisor-based tenant separation that has been strengthened and improved over two decades of Microsoft investments in Hyper-V technology for virtual machine isolation. The outcome of this approach is a robust Hypervisor that helps ensure tenant separation via 1) strongly defined security boundaries, 2) defense-in-depth exploits mitigations, and 3) strong security assurances processes.

Drawbridge isolation

For services that provide small units of processing using customer code, requests from multiple tenants are executed within a single VM and isolated using Microsoft [Drawbridge](#) technology. To provide security isolation, Drawbridge runs a user process together with a lightweight version of the Windows kernel (Library OS) inside a *pico-process*. A pico-process is a lightweight, secure isolation container with minimal kernel API surface and no direct access to services or resources of the Host system. The only external calls the pico-process can make are to the Drawbridge Security Monitor through the Drawbridge Application Binary Interface (ABI), as shown in Figure 8.

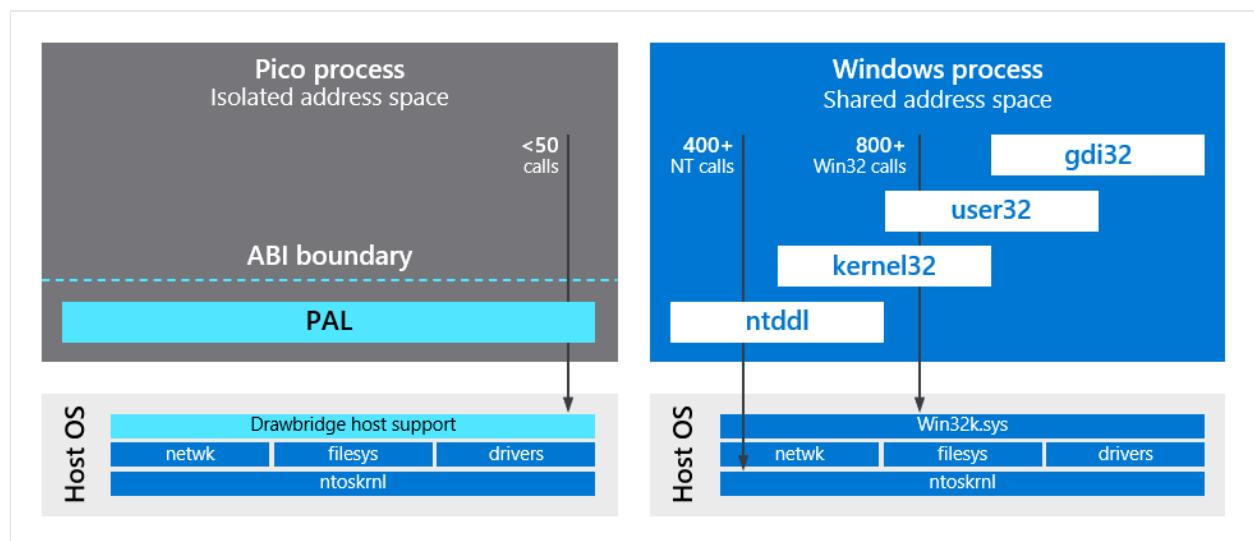


Figure 8. Process isolation using Drawbridge

The Security Monitor is divided into a system device driver and a user-mode component. The ABI is the interface between the Library OS and the Host. The entire interface consists of a closed set of fewer than 50 stateless function calls:

- Down calls from the pico-process to the Host OS support abstractions such as threads, virtual memory, and I/O streams.
- Up calls into the pico-process perform initialization, return exception information, and run in a new thread.

The semantics of the interface are fixed and support the general abstractions that applications require from any operating system. This design enables the Library OS and the Host to evolve separately.

The ABI is implemented within two components:

- The Platform Adaptation Layer (PAL) runs as part of the pico-process.
- The host implementation runs as part of the Host.

Pico-processes are grouped into isolation units called *sandboxes*. The sandbox defines the applications, file system, and external resources available to the pico-processes. When a process running inside a pico-process creates a new child process, it's run with its own Library OS in a separate pico-process inside the same sandbox. Each sandbox communicates to the Security Monitor, and isn't able to communicate with other sandboxes except via allowed I/O channels (sockets, named pipes, and so on), which need to be explicitly allowed by the configuration given the default opt-in approach depending on service needs. The outcome is that code running inside a pico-process can only access its own resources and can't directly attack the Host system or any colocated sandboxes. It's only able to affect objects inside its own sandbox.

When the pico-process needs system resources, it must call into the Drawbridge host to request them. The normal path for a virtual user process would be to call the Library OS to request resources and the Library OS would then call into the ABI. Unless the policy for resource allocation is set up in the driver itself, the Security Monitor would handle the ABI request by checking policy to see if the request is allowed and then servicing the request. This mechanism is used for all system primitives therefore ensuring that the code running in the pico-process can't abuse the resources from the Host machine.

In addition to being isolated inside sandboxes, pico-processes are also substantially isolated from each other. Each pico-process resides in its own virtual memory address space and runs its own copy of the Library OS with its own user-mode kernel. Each time a user process is launched in a Drawbridge sandbox, a fresh Library OS instance is booted. While this task is more time-consuming compared to launching a nonisolated process on Windows, it's substantially faster than booting a VM while accomplishing logical isolation.

A normal Windows process can call more than 1200 functions that result in access to the Windows kernel; however, the entire interface for a pico-process consists of fewer than

50 calls down to the Host. Most application requests for operating system services are handled by the Library OS within the address space of the pico-process. By providing a significantly smaller interface to the kernel, Drawbridge creates a more secure and isolated operating environment in which applications are much less vulnerable to changes in the Host system and incompatibilities introduced by new OS releases. More importantly, a Drawbridge pico-process is a strongly isolated container within which untrusted code from even the most malicious sources can be run without risk of compromising the Host system. The Host assumes that no code running within the pico-process can be trusted. The Host validates all requests from the pico-process with security checks.

Like a virtual machine, the pico-process is much easier to secure than a traditional OS interface because it's significantly smaller, stateless, and has fixed and easily described semantics. Another added benefit of the small ABI / driver syscall interface is the ability to audit / fuzz the driver code with little effort. For example, syscall fuzzers can fuzz the ABI with high coverage numbers in a relatively short amount of time.

User context-based isolation

In cases where an Azure service is composed of Microsoft-controlled code and customer code isn't allowed to run, the isolation is provided by a user context. These services accept only user configuration inputs and data for processing – arbitrary code isn't allowed. For these services, a user context is provided to establish the data that can be accessed and what Azure role-based access control (Azure RBAC) operations are allowed. This context is established by Microsoft Entra ID as described earlier in [*Identity-based isolation*](#) section. Once the user has been identified and authorized, the Azure service creates an application user context that is attached to the request as it moves through execution, providing assurance that user operations are separated and properly isolated.

Physical isolation

In addition to robust logical compute isolation available by design to all Azure tenants, if you desire physical compute isolation you can use Azure Dedicated Host or Isolated Virtual Machines, which are both dedicated to a single customer.

Note

Physical tenant isolation increases deployment cost and may not be required in most scenarios given the strong logical isolation assurances provided by Azure.

Azure Dedicated Host

Azure Dedicated Host provides physical servers that can host one or more Azure VMs and are dedicated to one Azure subscription. You can provision dedicated hosts within a region, availability zone, and fault domain. You can then place [Windows](#), [Linux](#), and [SQL Server on Azure](#) VMs directly into provisioned hosts using whatever configuration best meets your needs. Dedicated Host provides hardware isolation at the physical server level, enabling you to place your Azure VMs on an isolated and dedicated physical server that runs only your organization's workloads to meet corporate compliance requirements.

Note

You can deploy a dedicated host using the [Azure portal](#), [Azure PowerShell](#), and [Azure CLI](#).

You can deploy both Windows and Linux virtual machines into dedicated hosts by selecting the server and CPU type, number of cores, and extra features. Dedicated Host enables control over platform maintenance events by allowing you to opt in to a maintenance window to reduce potential impact to your provisioned services. Most maintenance events have little to no impact on your VMs; however, if you're in a highly regulated industry or with a sensitive workload, you may want to have control over any potential maintenance impact.

Microsoft provides detailed customer guidance on [Windows](#) and [Linux](#) Azure Virtual Machine provisioning using the Azure portal, Azure PowerShell, and Azure CLI. Table 5 summarizes the available security guidance for your virtual machines provisioned in Azure.

Table 5. Security guidance for Azure virtual machines

 Expand table

VM	Security guidance
Windows	Secure policies Azure Disk Encryption Built-in security controls Security recommendations
Linux	Secure policies Azure Disk Encryption

VM	Security guidance
	Built-in security controls Security recommendations

Isolated Virtual Machines

Azure Compute offers virtual machine sizes that are [isolated to a specific hardware type](#) and dedicated to a single customer. These VM instances allow your workloads to be deployed on dedicated physical servers. Using Isolated VMs essentially guarantees that your VM will be the only one running on that specific server node. You can also choose to further subdivide the resources on these Isolated VMs by using [Azure support for nested Virtual Machines](#).

Networking isolation

The logical isolation of tenant infrastructure in a public multi-tenant cloud is [fundamental to maintaining security](#). The overarching principle for a virtualized solution is to allow only connections and communications that are necessary for that virtualized solution to operate, blocking all other ports and connections by default. Azure [Virtual Network](#) (VNet) helps ensure that your private network traffic is logically isolated from traffic belonging to other customers. Virtual Machines (VMs) in one VNet can't communicate directly with VMs in a different VNet even if both VNets are created by the same customer. [Networking isolation](#) ensures that communication between your VMs remains private within a VNet. You can connect your VNets via [VNet peering](#) or [VPN gateways](#), depending on your connectivity options, including bandwidth, latency, and encryption requirements.

This section describes how Azure provides isolation of network traffic among tenants and enforces that isolation with cryptographic certainty.

Separation of tenant network traffic

Virtual networks (VNets) provide isolation of network traffic between tenants as part of their fundamental design. Your Azure subscription can contain multiple logically isolated private networks, and include firewall, load balancing, and network address translation. Each VNet is isolated from other VNets by default. Multiple deployments inside your subscription can be placed on the same VNet, and then communicate with each other through private IP addresses.

Network access to VMs is limited by packet filtering at the network edge, at load balancers, and at the Host OS level. Moreover, you can configure your host firewalls to further limit connectivity, specifying for each listening port whether connections are accepted from the Internet or only from role instances within the same cloud service or VNet.

Azure provides network isolation for each deployment and enforces the following rules:

- Traffic between VMs always traverses through trusted packet filters.
 - Protocols such as Address Resolution Protocol (ARP), Dynamic Host Configuration Protocol (DHCP), and other OSI Layer-2 traffic from a VM are controlled using rate-limiting and anti-spoofing protection.
 - VMs can't capture any traffic on the network that isn't intended for them.
- Your VMs can't send traffic to Azure private interfaces and infrastructure services, or to VMs belonging to other customers. Your VMs can only communicate with other VMs owned or controlled by you and with Azure infrastructure service endpoints meant for public communications.
- When you put a VM on a VNet, that VM gets its own address space that is invisible, and hence, not reachable from VMs outside of a deployment or VNet (unless configured to be visible via public IP addresses). Your environment is open only through the ports that you specify for public access; if the VM is defined to have a public IP address, then all ports are open for public access.

Packet flow and network path protection

Azure's hyperscale network is designed to provide:

- Uniform high capacity between servers.
- Performance isolation between services, including customers.
- Ethernet Layer-2 semantics.

Azure uses several networking implementations to achieve these goals:

- Flat addressing to allow service instances to be placed anywhere in the network.
- Load balancing to spread traffic uniformly across network paths.
- End-system based address resolution to scale to large server pools, without introducing complexity to the network control plane.

These implementations give each service the illusion that all the servers assigned to it, and only those servers, are connected by a single noninterfering Ethernet switch – a Virtual Layer 2 (VL2) – and maintain this illusion even as the size of each service varies from one server to hundreds of thousands. This VL2 implementation achieves traffic performance isolation, ensuring that it isn't possible for the traffic of one service to be

affected by the traffic of any other service, as if each service were connected by a separate physical switch.

This section explains how packets flow through the Azure network, and how the topology, routing design, and directory system combine to virtualize the underlying network fabric, creating the illusion that servers are connected to a large, noninterfering datacenter-wide Layer-2 switch.

The Azure network uses [two different IP-address families](#):

- **Customer address (CA)** is the customer defined/chosen VNet IP address, also referred to as Virtual IP (VIP). The network infrastructure operates using CAs, which are externally routable. All switches and interfaces are assigned CAs, and switches run an IP-based (Layer-3) link-state routing protocol that disseminates only these CAs. This design allows switches to obtain the complete switch-level topology, and forward packets encapsulated with CAs along shortest paths.
- **Provider address (PA)** is the Azure assigned internal fabric address that isn't visible to users and is also referred to as Dynamic IP (DIP). No traffic goes directly from the Internet to a server; all traffic from the Internet must go through a Software Load Balancer (SLB) and be encapsulated to protect the internal Azure address space by only routing packets to valid Azure internal IP addresses and ports. Network Address Translation (NAT) separates internal network traffic from external traffic. Internal traffic uses [RFC 1918](#) address space or private address space – the provider addresses (PAs) – that isn't externally routable. The translation is performed at the SLBs. Customer addresses (CAs) that are externally routable are translated into internal provider addresses (PAs) that are only routable within Azure. These addresses remain unaltered no matter how their servers' locations change due to virtual-machine migration or reprovisioning.

Each PA is associated with a CA, which is the identifier of the Top of Rack (ToR) switch to which the server is connected. VL2 uses a scalable, reliable directory system to store and maintain the mapping of PAs to CAs, and this mapping is created when servers are provisioned to a service and assigned PA addresses. An agent running in the network stack on every server, called the VL2 agent, invokes the directory system's resolution service to learn the actual location of the destination and then tunnels the original packet there.

Azure assigns servers IP addresses that act as names alone, with no topological significance. Azure's VL2 addressing scheme separates these server names (PAs) from their locations (CAs). The crux of offering Layer-2 semantics is having servers believe they share a single large IP subnet – that is, the entire PA space – with other servers in the same service, while eliminating the Address Resolution Protocol (ARP) and Dynamic

Host Configuration Protocol (DHCP) scaling bottlenecks that plague large Ethernet deployments.

Figure 9 depicts a sample packet flow where sender S sends packets to destination D via a randomly chosen intermediate switch using IP-in-IP encapsulation. PAs are from 20/8, and CAs are from 10/8. $H(ft)$ denotes a hash of the [5-tuple](#), which is composed of source IP, source port, destination IP, destination port, and protocol type. The ToR translates the PA to the CA, sends to the Intermediate switch, which sends to the destination CA ToR switch, which translates to the destination PA.

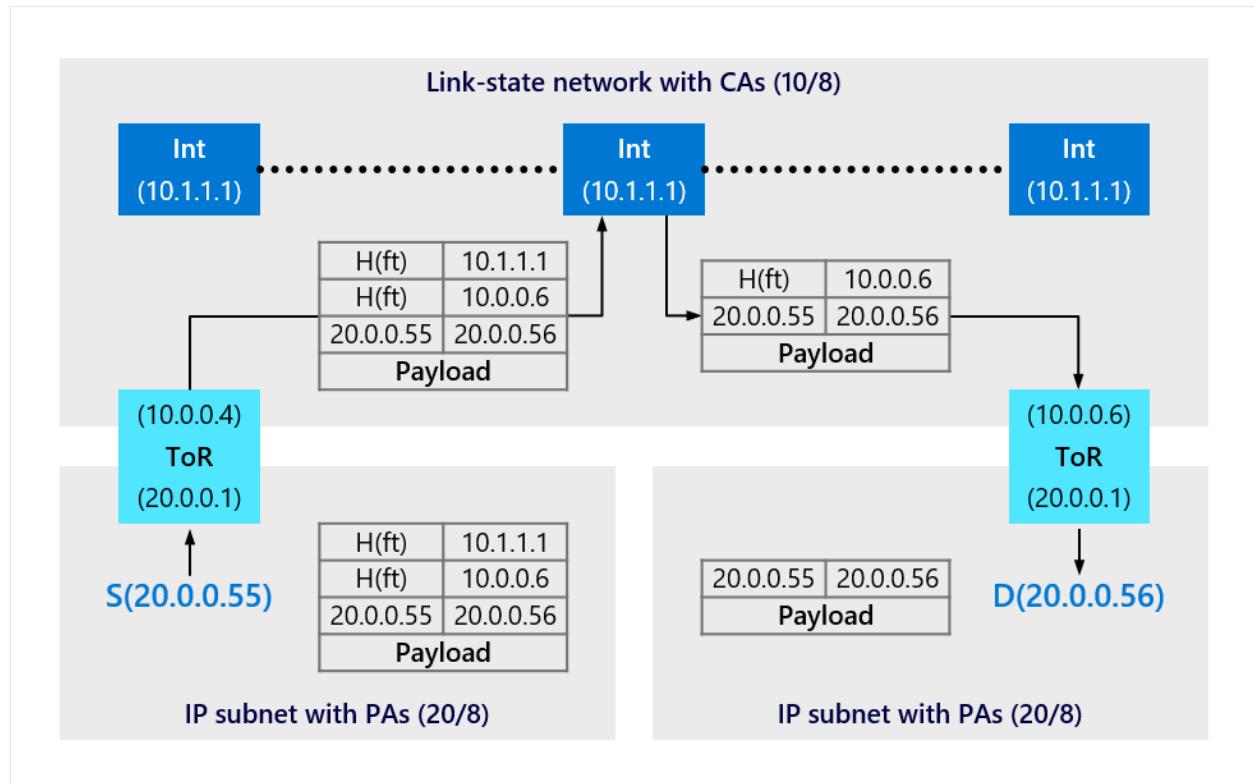


Figure 9. Sample packet flow

A server can't send packets to a PA if the directory service refuses to provide it with a CA through which it can route its packets, which means that the directory service enforces access control policies. Further, since the directory system knows which server is making the request when handling a lookup, it can **enforce fine-grained isolation policies**. For example, it can enforce a policy that only servers belonging to the same service can communicate with each other.

Traffic flow patterns

To route traffic between servers, which use PA addresses, on an underlying network that knows routes for CA addresses, the VL2 agent on each server captures packets from the host, and encapsulates them with the CA address of the ToR switch of the destination. Once the packet arrives at the CA (that is, the destination ToR switch), the destination ToR switch decapsulates the packet and delivers it to the destination PA carried in the

inner header. The packet is first delivered to one of the Intermediate switches, decapsulated by the switch, delivered to the ToR's CA, decapsulated again, and finally sent to the destination. This approach is depicted in Figure 10 using two possible traffic patterns: 1) external traffic (orange line) traversing over Azure ExpressRoute or the Internet to a VNet, and 2) internal traffic (blue line) between two VNets. Both traffic flows follow a similar pattern to isolate and protect network traffic.

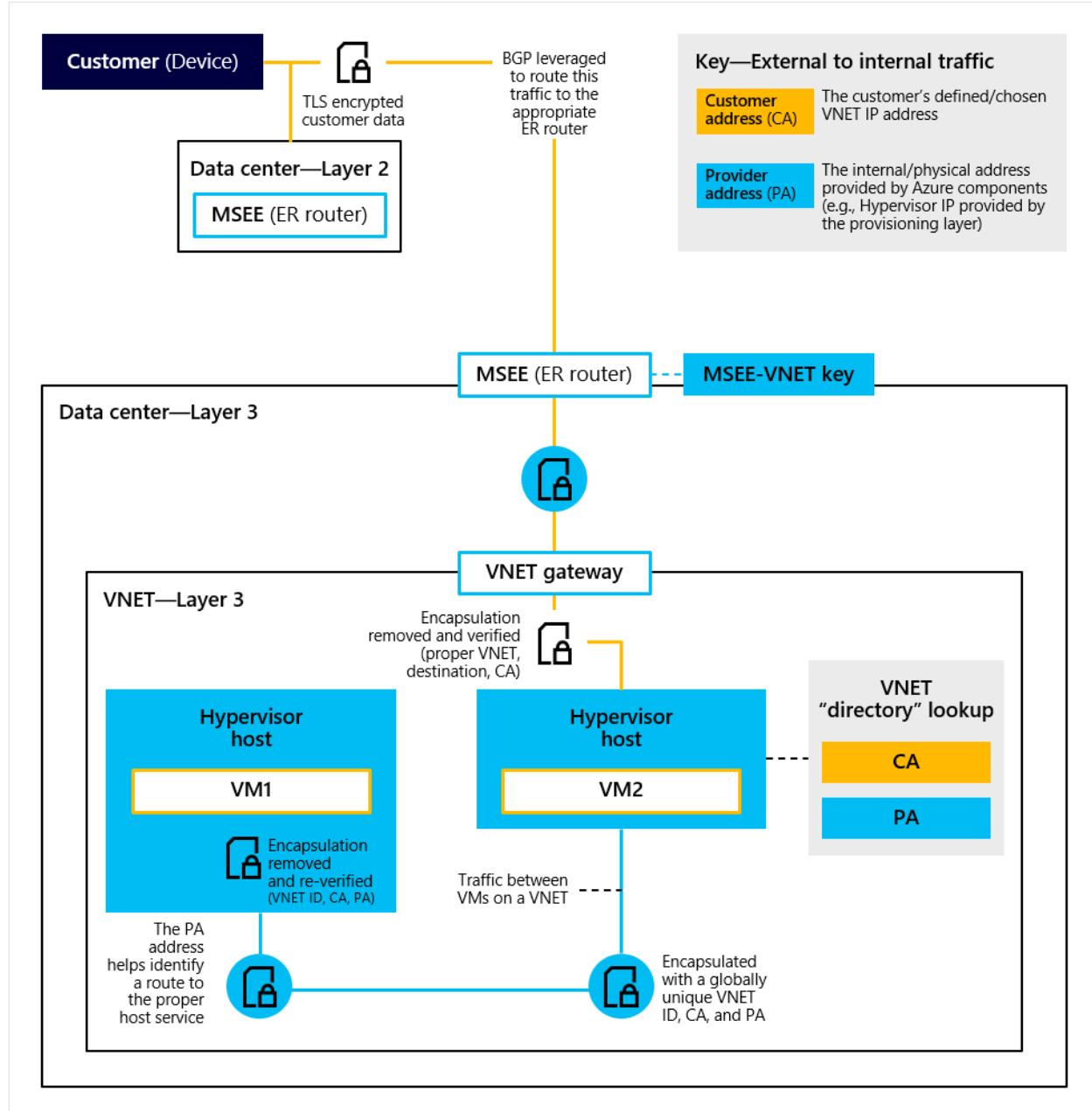


Figure 10. Separation of tenant network traffic using VNets

External traffic (orange line) – For external traffic, Azure provides multiple layers of assurance to enforce isolation depending on traffic patterns. When you place a public IP on your VNet gateway, traffic from the public Internet or your on-premises network that is destined for that IP address will be routed to an Internet Edge Router. Alternatively, when you establish private peering over an ExpressRoute connection, it's connected with an Azure VNet via VNet Gateway. This set-up aligns connectivity from the physical circuit and makes the private IP address space from the on-premises location

addressable. Azure then uses Border Gateway Protocol (BGP) to share routing details with the on-premises network to establish end-to-end connectivity. When communication begins with a resource within the VNet, the network traffic traverses as normal until it reaches a Microsoft ExpressRoute Edge (MSEE) Router. In both cases, VNets provide the means for Azure VMs to act as part of your on-premises network. A cryptographically protected [IPsec/IKE tunnel](#) is established between Azure and your internal network (for example, via [Azure VPN Gateway](#) or [Azure ExpressRoute Private Peering](#)), enabling the VM to connect securely to your on-premises resources as though it was directly on that network.

At the Internet Edge Router or the MSEE Router, the packet is encapsulated using Generic Routing Encapsulation (GRE). This encapsulation uses a unique identifier specific to the VNet destination and the destination address, which is used to appropriately route the traffic to the identified VNet. Upon reaching the VNet Gateway, which is a special VNet used only to accept traffic from outside of an Azure VNet, the encapsulation is verified by the Azure network fabric to ensure: a) the endpoint receiving the packet is a match to the unique VNet ID used to route the data, and b) the destination address requested exists in this VNet. Once verified, the packet is routed as internal traffic from the VNet Gateway to the final requested destination address within the VNet. This approach ensures that traffic from external networks travels only to Azure VNet for which it's destined, enforcing isolation.

Internal traffic (blue line) – Internal traffic also uses GRE encapsulation/tunneling. When two resources in an Azure VNet attempt to establish communications between each other, the Azure network fabric reaches out to the Azure VNet routing directory service that is part of the Azure network fabric. The directory services use the customer address (CA) and the requested destination address to determine the provider address (PA). This information, including the VNet identifier, CA, and PA, is then used to encapsulate the traffic with GRE. The Azure network uses this information to properly route the encapsulated data to the appropriate Azure host using the PA. The encapsulation is reviewed by the Azure network fabric to confirm:

1. The PA is a match,
2. The CA is located at this PA, and
3. The VNet identifier is a match.

Once all three are verified, the encapsulation is removed and routed to the CA as normal traffic, for example, to a VM endpoint. This approach provides VNet isolation assurance based on correct traffic routing between cloud services.

Azure VNets implement several mechanisms to ensure secure traffic between tenants. These mechanisms align to existing industry standards and security practices, and

prevent well-known attack vectors including:

- **Prevent IP address spoofing** – Whenever encapsulated traffic is transmitted by a VNet, the service reverifies the information on the receiving end of the transmission. The traffic is looked up and encapsulated independently at the start of the transmission, and reverified at the receiving endpoint to ensure the transmission was performed appropriately. This verification is done with an internal VNet feature called SpoofGuard, which verifies that the source and destination are valid and allowed to communicate, thereby preventing mismatches in expected encapsulation patterns that might otherwise permit spoofing. The GRE encapsulation processes prevent spoofing as any GRE encapsulation and encryption not done by the Azure network fabric is treated as dropped traffic.
- **Provide network segmentation across customers with overlapping network spaces** – Azure VNet's implementation relies on established tunneling standards such as the GRE, which in turn allows the use of customer-specific unique identifiers (VNet IDs) throughout the cloud. The VNet identifiers are used as scoping identifiers. This approach ensures that you're always operating within your unique address space, overlapping address spaces between tenants and the Azure network fabric. Anything that hasn't been encapsulated with a valid VNet ID is blocked within the Azure network fabric. In the example described previously, any encapsulated traffic not performed by the Azure network fabric is discarded.
- **Prevent traffic from crossing between VNets** – Preventing traffic from crossing between VNets is done through the same mechanisms that handle address overlap and prevent spoofing. Traffic crossing between VNets is rendered infeasible by using unique VNet IDs established per tenant in combination with verification of all traffic at the source and destination. Users don't have access to the underlying transmission mechanisms that rely on these IDs to perform the encapsulation. Therefore, any attempt to encapsulate and simulate these mechanisms would lead to dropped traffic.

In addition to these key protections, all unexpected traffic originating from the Internet is dropped by default. Any packet entering the Azure network will first encounter an Edge router. Edge routers intentionally allow all inbound traffic into the Azure network except spoofed traffic. This basic traffic filtering protects the Azure network from known bad malicious traffic. Azure also implements DDoS protection at the network layer, collecting logs to throttle or block traffic based on real time and historical data analysis, and mitigates attacks on demand.

Moreover, the Azure network fabric blocks traffic from any IPs originating in the Azure network fabric space that are spoofed. The Azure network fabric uses GRE and Virtual Extensible LAN (VXLAN) to validate that all allowed traffic is Azure-controlled traffic and all non-Azure GRE traffic is blocked. By using GRE tunnels and VXLAN to segment traffic

using customer unique keys, Azure meets [RFC 3809](#) and [RFC 4110](#). When using Azure VPN Gateway in combination with ExpressRoute, Azure meets [RFC 4111](#) and [RFC 4364](#). With a comprehensive approach for isolation encompassing external and internal network traffic, Azure VNets provide you with assurance that Azure successfully routes traffic between VNets, allows proper network segmentation for tenants with overlapping address spaces, and prevents IP address spoofing.

You're also able to use Azure services to further isolate and protect your resources. Using [network security groups](#) (NSGs), a feature of Azure Virtual Network, you can filter traffic by source and destination IP address, port, and protocol via multiple inbound and outbound security rules – essentially acting as a distributed virtual firewall and IP-based network access control list (ACL). You can apply an NSG to each NIC in a virtual machine, apply an NSG to the subnet that a NIC or another Azure resource is connected to, and directly to virtual machine scale set, allowing finer control over your infrastructure.

At the infrastructure layer, Azure implements a Hypervisor firewall to protect all tenants running within virtual machines on top of the Hypervisor from unauthorized access. This Hypervisor firewall is distributed as part of the NSG rules deployed to the Host, implemented in the Hypervisor, and configured by the Fabric Controller agent, as shown in Figure 4. The Host OS instances use the built-in Windows Firewall to implement fine-grained ACLs at a greater granularity than router ACLs – they're maintained by the same software that provisions tenants, so they're never out of date. The fine-grained ACLs are applied using the Machine Configuration File (MCF) to Windows Firewall.

At the top of the operating system stack is the Guest OS, which you use as your operating system. By default, this layer doesn't allow any inbound communication to cloud service or virtual network, essentially making it part of a private network. For PaaS Web and Worker roles, remote access isn't permitted by default. You can enable Remote Desktop Protocol (RDP) access as an explicit option. For IaaS VMs created using the Azure portal, RDP and remote PowerShell ports are opened by default; however, port numbers are assigned randomly. For IaaS VMs created via PowerShell, RDP and remote PowerShell ports must be opened explicitly. If the administrator chooses to keep the RDP and remote PowerShell ports open to the Internet, the account allowed to create RDP and PowerShell connections should be secured with a strong password. Even if ports are open, you can define ACLs on the public IPs for extra protection if desired.

Service tags

You can use Virtual Network [service tags](#) to achieve network isolation and protect your Azure resources from the Internet while accessing Azure services that have public endpoints. With service tags, you can define network access controls on [network security groups](#) or [Azure Firewall](#). A service tag represents a group of IP address prefixes

from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, thereby reducing the complexity of frequent updates to network security rules.

ⓘ Note

You can create inbound/outbound network security group rules to deny traffic to/from the Internet and allow traffic to/from Azure. Service tags are available for many Azure services for use in network security group rules.

Extra resources:

- [Available service tags for specific Azure services](#)

Azure Private Link

You can use [Private Link](#) to access Azure PaaS services and Azure-hosted customer/partner services over a [private endpoint](#) in your VNet, ensuring that traffic between your VNet and the service travels across the Microsoft global backbone network. This approach eliminates the need to expose the service to the public Internet. You can also create your own [private link service](#) in your own VNet and deliver it to your customers.

Azure private endpoint is a network interface that connects you privately and securely to a service powered by Private Link. Private endpoint uses a private IP address from your VNet, effectively bringing the service into your VNet.

From the networking isolation standpoint, key benefits of Private Link include:

- You can connect your VNet to services in Azure without a public IP address at the source or destination. Private Link handles the connectivity between the service and its consumers over the Microsoft global backbone network.
- You can access services running in Azure from on-premises over Azure ExpressRoute private peering, VPN tunnels, and peered virtual networks using private endpoints. Private Link eliminates the need to set up public peering or traverse the Internet to reach the service.
- You can connect privately to services running in other Azure regions.

ⓘ Note

You can use the Azure portal to manage private endpoint connections on Azure PaaS resources. For customer/partner owned Private Link services, Azure Power

Shell and Azure CLI are the preferred methods for managing private endpoint connections.

Extra resources:

- [How to manage private endpoint connections on Azure PaaS resources](#)
- [How to manage private endpoint connections on a customer- or partner-owned Private Link service](#)

Data encryption in transit

Azure provides many options for [encrypting data in transit](#). Data encryption in transit isolates your network traffic from other traffic and helps protect data from interception. Data in transit applies to scenarios involving data traveling between:

- Your end users and Azure service
- Your on-premises datacenter and Azure region
- Microsoft datacenters as part of expected Azure service operation

End user's connection to Azure service

Transport Layer Security (TLS) – Azure uses the TLS protocol to help protect data when it's traveling between your end users and Azure services. Most of your end users will connect to Azure over the Internet, and the precise routing of network traffic will depend on the many network providers that contribute to Internet infrastructure. As stated in the Microsoft Products and Services [Data Protection Addendum](#) (DPA), Microsoft doesn't control or limit the regions from which you or your end users may access or move customer data.

Important

You can increase security by enabling encryption in transit. For example, you can use [Application Gateway](#) to configure [end-to-end encryption](#) of network traffic and rely on [Key Vault integration](#) for TLS termination.

Across Azure services, traffic to and from the service is [protected by TLS 1.2](#) using RSA-2048 for key exchange and AES-256 for data encryption. The corresponding crypto modules are FIPS 140 validated as part of the Microsoft [Windows FIPS validation program](#).

TLS provides strong authentication, message privacy, and integrity. [Perfect Forward Secrecy](#) (PFS) protects connections between your client systems and Microsoft cloud services by generating a unique session key for every session you initiate. PFS protects past sessions against potential future key compromises. This combination makes it more difficult to intercept and access data in transit.

In-transit encryption for VMs – Remote sessions to Windows and Linux VMs deployed in Azure can be conducted over protocols that ensure data encryption in transit. For example, the [Remote Desktop Protocol](#) (RDP) initiated from your client computer to Windows and Linux VMs enables TLS protection for data in transit. You can also use [Secure Shell](#) (SSH) to connect to Linux VMs running in Azure. SSH is an encrypted connection protocol available by default for remote management of Linux VMs hosted in Azure.

ⓘ Important

You should review best practices for network security, including guidance for [disabling RDP/SSH access to Virtual Machines](#) from the Internet to mitigate brute force attacks to gain access to Azure Virtual Machines. Accessing VMs for remote management can then be accomplished via [point-to-site VPN](#), [site-to-site VPN](#), or [Azure ExpressRoute](#).

Azure Storage transactions – When interacting with Azure Storage through the Azure portal, all transactions take place over HTTPS. Moreover, you can configure your storage accounts to accept requests only from secure connections by setting the “[secure transfer required](#)” property for the storage account. The “secure transfer required” option is enabled by default when creating a Storage account in the Azure portal.

[Azure Files](#) offers fully managed file shares in the cloud that are accessible via the industry-standard [Server Message Block](#) (SMB) protocol. By default, all Azure storage accounts [have encryption in transit enabled](#). Therefore, when mounting a share over SMB or accessing it through the Azure portal (or Azure PowerShell, Azure CLI, and Azure SDKs), Azure Files will only allow the connection if it's made with SMB 3.0+ with encryption or over HTTPS.

Datacenter connection to Azure region

VPN encryption – [Virtual Network](#) (VNet) provides a means for Azure Virtual Machines (VMs) to act as part of your internal (on-premises) network. With VNet, you choose the address ranges of non-globally-routable IP addresses to be assigned to the VMs so that

they won't collide with addresses you're using elsewhere. You have options to securely connect to a VNet from your on-premises infrastructure or remote locations.

- **Site-to-Site** (IPsec/IKE VPN tunnel) – A cryptographically protected “tunnel” is established between Azure and your internal network, allowing an Azure VM to connect to your back-end resources as though it was directly on that network. This type of connection requires a [VPN device](#) located on-premises that has an externally facing public IP address assigned to it. You can use Azure [VPN Gateway](#) to send encrypted traffic between your VNet and your on-premises infrastructure across the public Internet, for example, a [site-to-site VPN](#) relies on IPsec for transport encryption. VPN Gateway supports many encryption algorithms that are FIPS 140 validated. Moreover, you can configure VPN Gateway to use [custom IPsec/IKE policy](#) with specific cryptographic algorithms and key strengths instead of relying on the default Azure policies. IPsec encrypts data at the IP level (Network Layer 3).
- **Point-to-Site** (VPN over SSTP, OpenVPN, and IPsec) – A secure connection is established from your individual client computer to your VNet using Secure Socket Tunneling Protocol (SSTP), OpenVPN, or IPsec. As part of the [Point-to-Site VPN](#) configuration, you need to install a certificate and a VPN client configuration package, which allow the client computer to connect to any VM within the VNet. [Point-to-Site VPN](#) connections don't require a VPN device or a public facing IP address.

In addition to controlling the type of algorithm that is supported for VPN connections, Azure provides you with the ability to enforce that all traffic leaving a VNet may only be routed through a VNet Gateway (for example, Azure VPN Gateway). This enforcement allows you to ensure that traffic may not leave a VNet without being encrypted. A VPN Gateway can be used for [VNet-to-VNet](#) connections while also providing a secure tunnel with IPsec/IKE. Azure VPN uses [Pre-Shared Key \(PSK\) authentication](#) whereby Microsoft generates the PSK when the VPN tunnel is created. You can change the autogenerated PSK to your own.

Azure ExpressRoute encryption – [Azure ExpressRoute](#) allows you to create private connections between Microsoft datacenters and your on-premises infrastructure or colocation facility. ExpressRoute connections don't go over the public Internet and offer lower latency and higher reliability than IPsec protected VPN connections. [ExpressRoute locations](#) are the entry points to Microsoft's global network backbone and they may or may not match the location of Azure regions. Once the network traffic enters the Microsoft backbone, it's guaranteed to traverse that private networking infrastructure instead of the public Internet. You can use ExpressRoute with several data [encryption options](#), including [MACsec](#) that enable you to store [MACsec encryption keys](#) in Azure [Key Vault](#). MACsec encrypts data at the Media Access Control (MAC) level, that is, data

link layer (Network Layer 2). Both AES-128 and AES-256 block ciphers are [supported for encryption](#). You can use MACsec to encrypt the physical links between your network devices and Microsoft network devices when you connect to Microsoft via [ExpressRoute Direct](#). ExpressRoute Direct allows for direct fiber connections from your edge to the Microsoft Enterprise edge routers at the peering locations.

You can enable IPsec in addition to MACsec on your ExpressRoute Direct ports, as shown in Figure 11. Using VPN Gateway, you can set up an [IPsec tunnel over Microsoft Peering](#) of your ExpressRoute circuit between your on-premises network and your Azure VNet. MACsec secures the physical connection between your on-premises network and Microsoft. IPsec secures the end-to-end connection between your on-premises network and your VNets in Azure. MACsec and IPsec can be enabled independently.

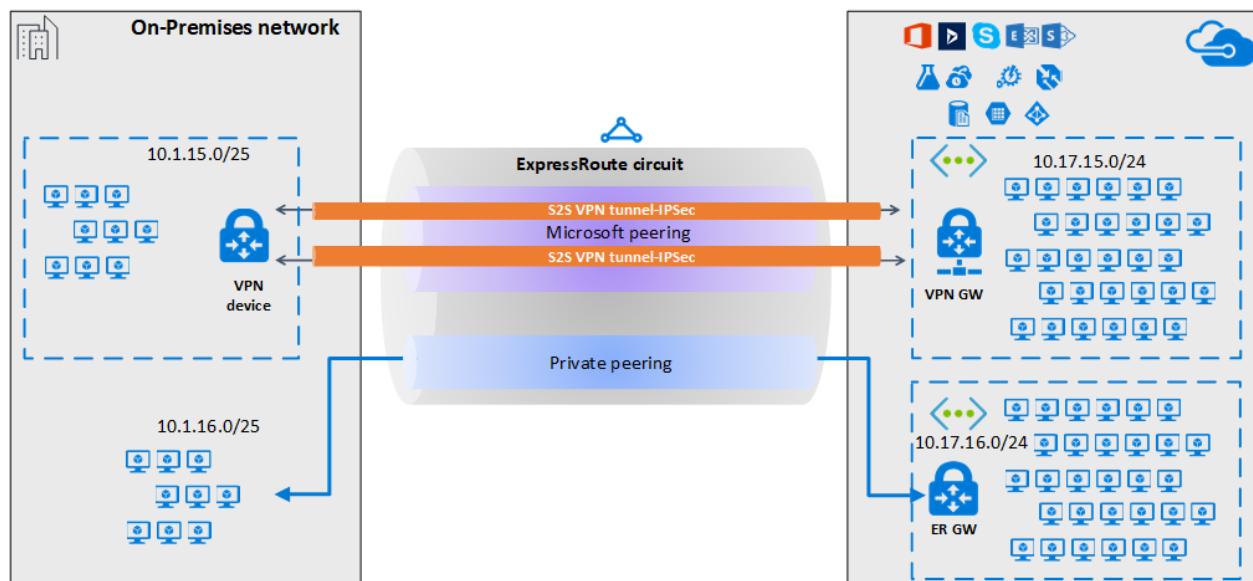


Figure 11. VPN and ExpressRoute encryption for data in transit

Traffic across Microsoft global network backbone

Azure services such as Storage and SQL Database can be configured for geo-replication to help ensure durability and high availability especially for disaster recovery scenarios. Azure relies on [paired regions](#) to deliver [geo-redundant storage](#) (GRS) and paired regions are also recommended when configuring active [geo-replication](#) for Azure SQL Database. Paired regions are located within the same geography; however, network traffic isn't guaranteed to always follow the same path from one Azure region to another. To provide the reliability needed for the Azure cloud, Microsoft has many physical networking paths with automatic routing around failures for optimal reliability.

Moreover, all Azure traffic traveling within a region or between regions is [encrypted by Microsoft using MACsec](#), which relies on AES-128 block cipher for encryption. This traffic stays entirely within the Microsoft [global network backbone](#) and never enters the public

Internet. The backbone is one of the largest in the world with more than 250,000 km of lit fiber optic and undersea cable systems.

Important

You should review Azure [best practices for the protection of data in transit](#) to help ensure that all data in transit is encrypted. For key Azure PaaS storage services (for example, Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics), data encryption in transit is [enforced by default](#).

Third-party network virtual appliances

Azure provides you with many features to help you achieve your security and isolation goals, including [Microsoft Defender for Cloud](#), [Azure Monitor](#), [Azure Firewall](#), [VPN Gateway](#), [network security groups](#), [Application Gateway](#), [Azure DDoS Protection](#), [Network Watcher](#), [Microsoft Sentinel](#), and [Azure Policy](#). In addition to the built-in capabilities that Azure provides, you can use third-party [network virtual appliances](#) to accommodate your specific network isolation requirements while at the same time applying existing in-house skills. Azure supports many appliances, including offerings from F5, Palo Alto Networks, Cisco, Check Point, Barracuda, Citrix, Fortinet, and many others. Network appliances support network functionality and services in the form of VMs in your virtual networks and deployments.

The cumulative effect of network isolation restrictions is that each cloud service acts as though it were on an isolated network where VMs within the cloud service can communicate with one another, identifying one another by their source IP addresses with confidence that no other parties can impersonate their peer VMs. They can also be configured to accept incoming connections from the Internet over specific ports and protocols and to ensure that all network traffic leaving your virtual networks is always encrypted.

Tip

You should review published Azure networking documentation for guidance on how to use native security features to help protect your data.

Extra resources:

- [Azure network security overview](#)
- [Azure network security](#)

Storage isolation

Microsoft Azure separates your VM-based compute resources from storage as part of its [fundamental design](#). The separation allows compute and storage to scale independently, making it easier to provide multi-tenancy and isolation. Therefore, Azure Storage runs on separate hardware with no network connectivity to Azure Compute except logically.

Each Azure [subscription](#) can have one or more storage accounts. Azure storage supports various [authentication options](#), including:

- **Shared symmetric keys** – Upon storage account creation, Azure generates two 512-bit storage account keys that control access to the storage account. You can rotate and regenerate these keys at any point thereafter without coordination with your applications.
- **Microsoft Entra ID-based authentication** – Access to Azure Storage can be controlled by Microsoft Entra ID, which enforces tenant isolation and implements robust measures to prevent access by unauthorized parties, including Microsoft insiders. More information about Microsoft Entra tenant isolation is available from a white paper [Microsoft Entra Data Security Considerations](#) ↗.
- **Shared access signatures (SAS)** – Shared access signatures or “presigned URLs” can be created from the shared symmetric keys. These URLs can be significantly limited in scope to reduce the available attack surface, but at the same time allow applications to grant storage access to another user, service, or device.
- **User delegation SAS** – Delegated authentication is similar to SAS but is [based on Microsoft Entra tokens](#) rather than the shared symmetric keys. This approach allows a service that authenticates with Microsoft Entra ID to create a pre signed URL with limited scope and grant temporary access to another user, service, or device.
- **Anonymous public read access** – You can allow a small portion of your storage to be publicly accessible without authentication or authorization. This capability can be disabled at the subscription level if you desire more stringent control.

Azure Storage provides storage for a wide variety of workloads, including:

- Azure Virtual Machines (disk storage)
- Big data analytics (HDFS for HDInsight, Azure Data Lake Storage)
- Storing application state, user data (Blob, Queue, Table storage)
- Long-term data storage (Azure Archive Storage)
- Network file shares in the cloud (File storage)
- Serving web pages on the Internet (static websites)

While Azure Storage supports many different externally facing customer storage scenarios, internally, the physical storage for the above services is managed by a common set of APIs. To provide durability and availability, Azure Storage relies on data replication and data partitioning across storage resources that are shared among tenants. To ensure cryptographic certainty of logical data isolation, Azure Storage relies on data encryption at rest using advanced algorithms with multiple ciphers as described in this section.

Data replication

Your data in an Azure Storage account is [always replicated](#) to help ensure durability and high availability. Azure Storage copies your data to protect it from transient hardware failures, network or power outages, and even massive natural disasters. You can typically choose to replicate your data within the same data center, across [availability zones within the same region](#), or across geographically separated regions. Specifically, when creating a storage account, you can select one of the following [redundancy options](#):

- **Locally redundant storage (LRS)** replicates three copies (or the erasure coded equivalent, as described later) of your data within a single data center. A write request to an LRS storage account returns successfully only after the data is written to all three replicas. Each replica resides in separate fault and upgrade domains within a scale unit (set of storage racks within a data center).
- **Zone-redundant storage (ZRS)** replicates your data synchronously across three storage clusters in a single [region](#). Each storage cluster is physically separated from the others and is in its own [Availability Zone](#) (AZ). A write request to a ZRS storage account returns successfully only after the data is written to all replicas across the three clusters.
- **Geo-redundant storage (GRS)** replicates your data to a [secondary \(paired\) region](#) that is hundreds of kilometers away from the primary region. GRS storage accounts are durable even during a complete regional outage or a disaster in which the primary region isn't recoverable. For a storage account with GRS or RA-GRS enabled, all data is first replicated with LRS. An update is first committed to the primary location and replicated using LRS. The update is then replicated asynchronously to the secondary region using GRS. When data is written to the secondary location, it's also replicated within that location using LRS.
- **Read-access geo-redundant storage (RA-GRS)** is based on GRS. It provides read-only access to the data in the secondary location, in addition to geo-replication across two regions. With RA-GRS, you can read from the secondary region regardless of whether Microsoft initiates a failover from the primary to secondary region.

- **Geo-zone-redundant storage (GZRS)** combines the high availability of ZRS with protection from regional outages as provided by GRS. Data in a GZRS storage account is replicated across three AZs in the primary region and also replicated to a secondary geographic region for protection from regional disasters. Each Azure region is paired with another region within the same geography, together making a [regional pair](#).
- **Read-access geo-zone-redundant storage (RA-GZRS)** is based on GZRS. You can optionally enable read access to data in the secondary region with RA-GZRS if your applications need to be able to read data following a disaster in the primary region.

High-level Azure Storage architecture

Azure Storage production systems consist of storage stamps and the location service (LS), as shown in Figure 12. A storage stamp is a cluster of racks of storage nodes, where each rack is built as a separate fault domain with redundant networking and power. The LS manages all the storage stamps and the account namespace across all stamps. It allocates accounts to storage stamps and manages them across the storage stamps for load balancing and disaster recovery. The LS itself is distributed across two geographic locations for its own disaster recovery ([Calder, et al., 2011](#) ↗).

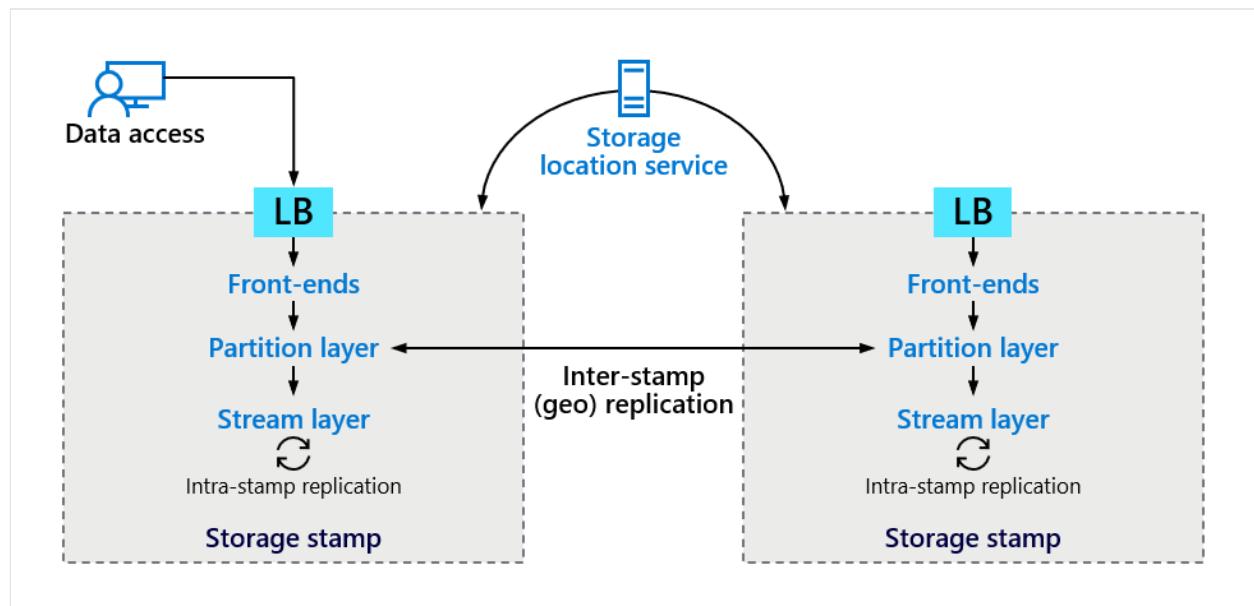


Figure 12. High-level Azure Storage architecture (Source: [Calder, et al., 2011](#) ↗)

There are three layers within a storage stamp: front-end, partition, and stream. These layers are described in the rest of this section.

Front-end layer

The front-end (FE) layer consists of a set of stateless servers that take the incoming requests, authenticate and authorize the requests, and then route them to a partition server in the Partition Layer. The FE layer knows what partition server to forward each request to, since each front-end server caches a partition map. The partition map keeps track of the partitions for the service being accessed and what partition server is controlling (serving) access to each partition in the system. The FE servers also stream large objects directly from the stream layer.

Transferring large volumes of data across the Internet is inherently unreliable. Using Azure block blobs service, you can upload and store large files efficiently by breaking up large files into smaller blocks of data. In this manner, block blobs allow partitioning of data into individual blocks for reliability of large uploads, as shown in Figure 13. Each block can be up to 100 MB in size with up to 50,000 blocks in the block blob. If a block fails to transmit correctly, only that particular block needs to be resent versus having to resend the entire file again. In addition, with a block blob, multiple blocks can be sent in parallel to decrease upload time.

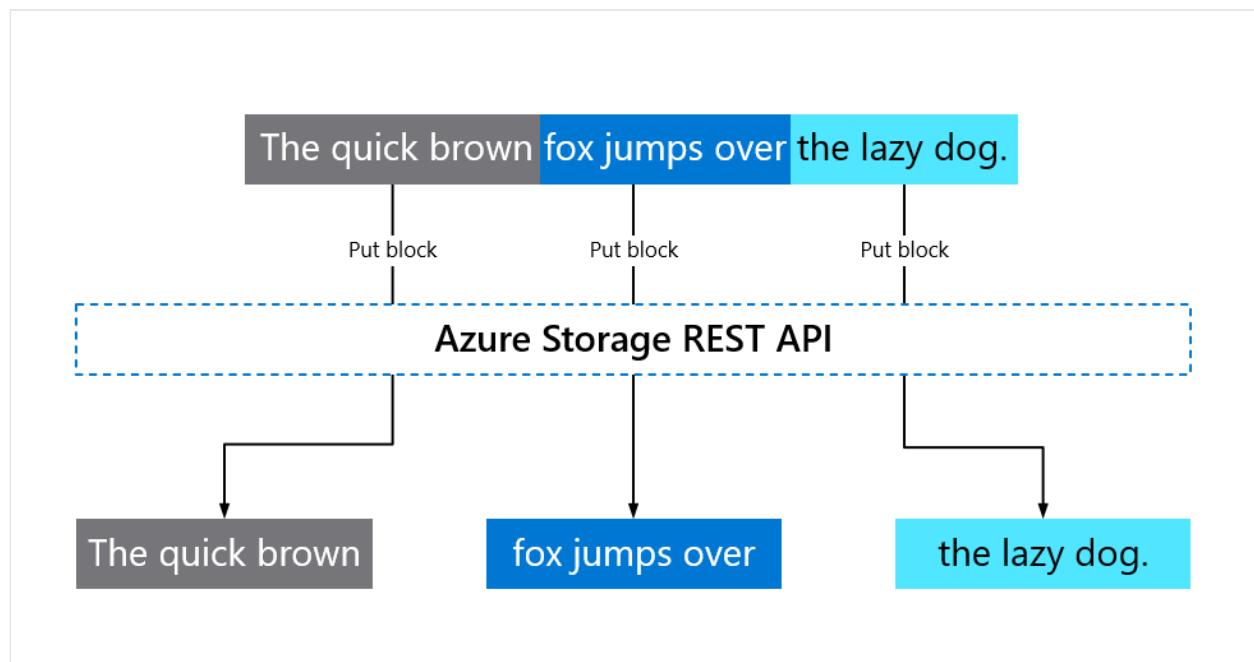


Figure 13. Block blob partitioning of data into individual blocks

You can upload blocks in any order and determine their sequence in the final blocklist commitment step. You can also upload a new block to replace an existing uncommitted block of the same block ID.

Partition layer

The partition layer is responsible for:

- Managing higher-level data abstractions (Blob, Table, Queue),
- Providing a scalable object namespace,

- Providing transaction ordering and strong consistency for objects,
- Storing object data on top of the stream layer, and
- Caching object data to reduce disk I/O.

This layer also provides asynchronous geo-replication of data and is focused on replicating data across stamps. Inter-stamp replication is done in the background to keep a copy of the data in two locations for disaster recovery purposes.

Once a blob is ingested by the FE layer, the partition layer is responsible for tracking and storing where data is placed in the stream layer. Each storage tenant can have approximately 200 - 300 individual partition layer nodes, and each node is responsible for tracking and serving a partition of the data stored in that Storage tenant. The high throughput block blob (HTBB) feature enables data to be sharded within a single blob, which allows the workload for large blobs to be shared across multiple partition layer servers (Figure 14). Distributing the load among multiple partition layer servers greatly improves availability, throughput, and durability.

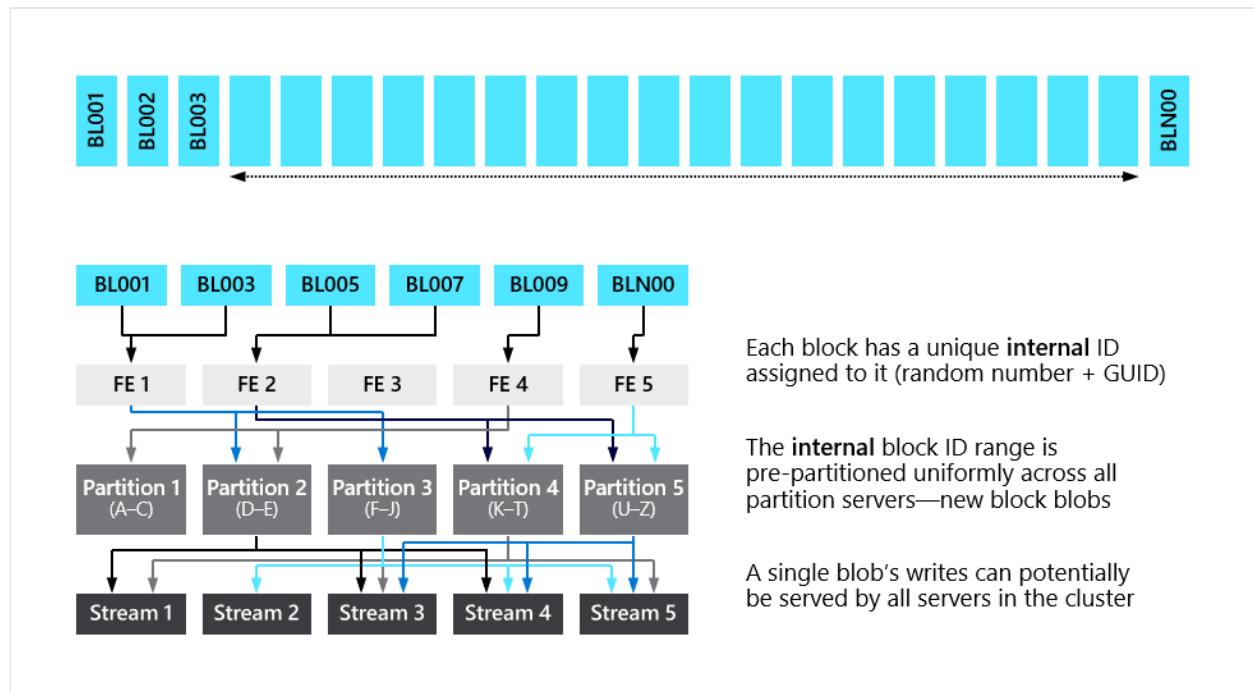


Figure 14. High throughput block blobs spread traffic and data across multiple partition servers and streams

Stream layer

The stream layer stores the bits on disk, and is responsible for distributing and replicating the data across many servers to keep data durable within a storage stamp. It acts as a distributed file system layer within a stamp. It handles files, called streams, which are ordered lists of data blocks called extents that are analogous to extents on physical hard drives. Large blob objects can be stored in multiple extents, potentially on multiple physical extent nodes (ENs). The data is stored in the stream layer, but it's

accessible from the partition layer. Partition servers and stream servers are colocated on each storage node in a stamp.

The stream layer provides synchronous replication (intra-stamp) across different nodes in different fault domains to keep data durable within the stamp. It's responsible for creating the three local replicated copies of each extent. The stream layer manager makes sure that all three copies are distributed across different physical racks and nodes on different fault and upgrade domains so that copies are resilient to individual disk/node/rack failures and planned downtime due to upgrades.

Erasure Coding – Azure Storage uses a technique called [Erasure Coding](#), which allows for the reconstruction of data even if some of the data is missing due to disk failure. This approach is similar to the concept of RAID striping for individual disks where data is spread across multiple disks so that if a disk is lost, the missing data can be reconstructed using the parity bits from the data on the other disks. Erasure Coding splits an extent into equal data and parity fragments that are stored on separate ENs, as shown in Figure 15.

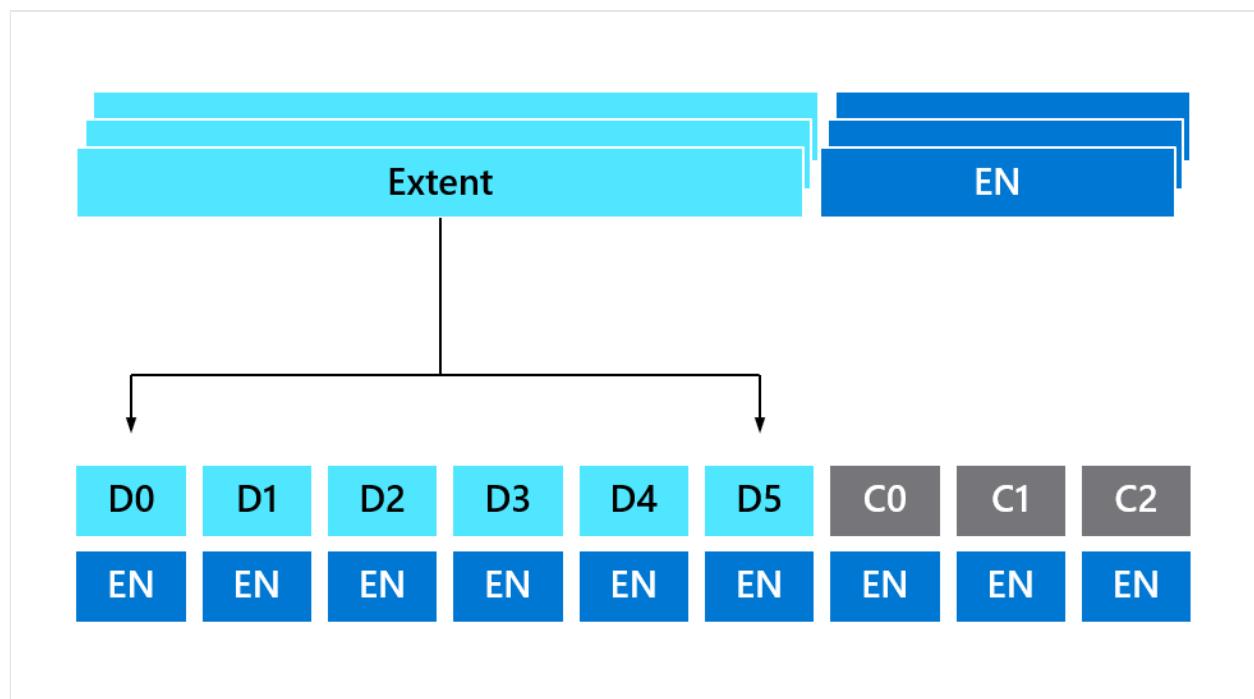


Figure 15. Erasure Coding further shards extent data across EN servers to protect against failure

All data blocks stored in stream extent nodes have a 64-bit cyclic redundancy check (CRC) and a header protected by a hash signature to provide extent node (EN) data integrity. The CRC and signature are checked before every disk write, disk read, and network receive. In addition, scrubber processes read all data at regular intervals verifying the CRC and looking for *bit rot*. If a bad extent is found a new copy of that extent is created to replace the bad extent.

Your data in Azure Storage relies on data encryption at rest to provide cryptographic certainty for logical data isolation. You can choose between Microsoft-managed encryption keys (also known as platform-managed encryption keys) or customer-managed encryption keys (CMK). The handling of data encryption and decryption is transparent to customers, as discussed in the next section.

Data encryption at rest

Azure provides extensive options for [data encryption at rest](#) to help you safeguard your data and meet your compliance needs when using both Microsoft-managed encryption keys and customer-managed encryption keys. For more information, see [data encryption models](#). This process relies on multiple encryption keys and services such as Azure Key Vault and Microsoft Entra ID to ensure secure key access and centralized key management.

Note

If you require extra security and isolation assurances for your most sensitive data stored in Azure services, you can encrypt it using your own encryption keys you control in Azure Key Vault.

In general, controlling key access and ensuring efficient bulk encryption and decryption of data is accomplished via the following types of encryption keys (as shown in Figure 16), although other encryption keys can be used as described in [Storage service encryption](#) section.

- **Data Encryption Key (DEK)** is a symmetric AES-256 key that is used for bulk encryption and decryption of a partition or a block of data. The cryptographic modules are FIPS 140 validated as part of the [Windows FIPS validation program](#). Access to DEKs is needed by the resource provider or application instance that is responsible for encrypting and decrypting a specific block of data. A single resource may have many partitions and many DEKs. When a DEK is replaced with a new key, only the data in its associated block must be re-encrypted with the new key. The DEK is always stored encrypted by the Key Encryption Key (KEK).
- **Key Encryption Key (KEK)** is an asymmetric RSA key that is optionally provided by you. This key encryption key is utilized to encrypt the Data Encryption Key (DEK) using Azure Key Vault or Managed HSM. As mentioned previously in [Data encryption key management](#) section, Azure Key Vault can use FIPS 140 validated hardware security modules (HSMs) to safeguard encryption keys; Managed HSM always uses FIPS 140 validated hardware security modules. These keys aren't exportable and there can be no clear-text version of the KEK outside the HSMs –

the binding is enforced by the underlying HSM. KEK is never exposed directly to the resource provider or other services. Access to KEK is controlled by permissions in Azure Key Vault and access to Azure Key Vault must be authenticated through Microsoft Entra ID. These permissions can be revoked to block access to this key and, by extension, the data that is encrypted using this key as the root of the key chain.

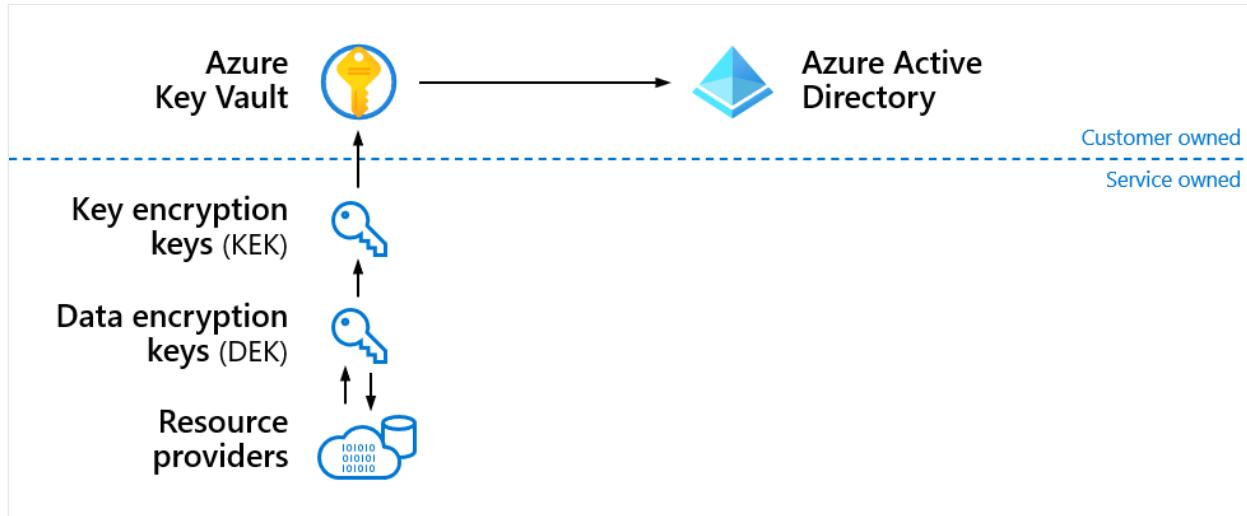


Figure 16. Data Encryption Keys are encrypted using your key stored in Azure Key Vault

Therefore, the encryption key hierarchy involves both DEK and KEK. DEK is encrypted with KEK and stored separately for efficient access by resource providers in bulk encryption and decryption operations. However, only an entity with access to the KEK can decrypt the DEK. The entity that has access to the KEK may be different than the entity that requires the DEK. Since the KEK is required to decrypt the DEK, the KEK is effectively a single point by which DEK can be deleted via deletion of the KEK.

Detailed information about various [data encryption models](#) and specifics on key management for many Azure platform services is available in online documentation. Moreover, some Azure services provide other [encryption models](#), including client-side encryption, to further encrypt their data using more granular controls. The rest of this section covers encryption implementation for key Azure storage scenarios such as Storage service encryption and disk encryption for IaaS Virtual Machines.

💡 Tip

You should review published Azure data encryption documentation for guidance on how to protect your data.

Extra resources:

- [Encryption at rest overview](#)
- [Data encryption models](#)

- **Data encryption best practices**

Storage service encryption

Azure [Storage service encryption](#) for data at rest ensures that data is automatically encrypted before persisting it to Azure Storage and decrypted before retrieval. All data written to Azure Storage is encrypted through FIPS 140 validated 256-bit AES encryption, and the handling of encryption, decryption, and key management in Storage service encryption is transparent to customers. By default, Microsoft controls the encryption keys and is responsible for key rotation, usage, and access. Keys are stored securely and protected inside a Microsoft key store. This option provides you with the most convenience given that all Azure Storage services are supported.

However, you can also choose to manage encryption with your own keys by specifying:

- [Customer-managed key](#) for managing Azure Storage encryption whereby the key is stored in Azure Key Vault. This option provides much flexibility for you to create, rotate, disable, and revoke access to customer-managed keys. You must use Azure Key Vault to store customer-managed keys. Both key vaults and managed HSMs are supported, as described previously in [Azure Key Vault](#) section.
- [Customer-provided key](#) for encrypting and decrypting Blob storage only whereby the key can be stored in Azure Key Vault or in another key store on your premises to meet regulatory compliance requirements. Customer-provided keys enable you to pass an encryption key to Storage service using Blob APIs as part of read or write operations.

Note

You can configure customer-managed keys (CMK) with Azure Key Vault using the [Azure portal](#), [Azure PowerShell](#), or [Azure CLI](#). You can use [.NET](#) to specify a customer-provided key on a request to Blob storage.

Storage service encryption is enabled by default for all new and existing storage accounts and it [can't be disabled](#). As shown in Figure 17, the encryption process uses the following keys to help ensure cryptographic certainty of data isolation at rest:

- *Data Encryption Key (DEK)* is a symmetric AES-256 key that is used for bulk encryption, and it's unique per storage account in Azure Storage. It's generated by the Azure Storage service as part of the storage account creation and is used to derive a unique key for each block of data. The Storage Service always encrypts the

DEK using either the Stamp Key or a Key Encryption Key if the customer has configured customer-managed key encryption.

- *Key Encryption Key (KEK)* is an asymmetric RSA (2048 or greater) key managed by the customer and is used to encrypt the Data Encryption Key (DEK) using Azure Key Vault or Managed HSM. It's never exposed directly to the Azure Storage service or other services.
- *Stamp Key (SK)* is a symmetric AES-256 key managed by Azure Storage. This key is used to protect the DEK when not using a customer-managed key.

These keys protect any data that is written to Azure Storage and provide cryptographic certainty for logical data isolation in Azure Storage. As mentioned previously, Azure Storage service encryption is enabled by default and it can't be disabled.

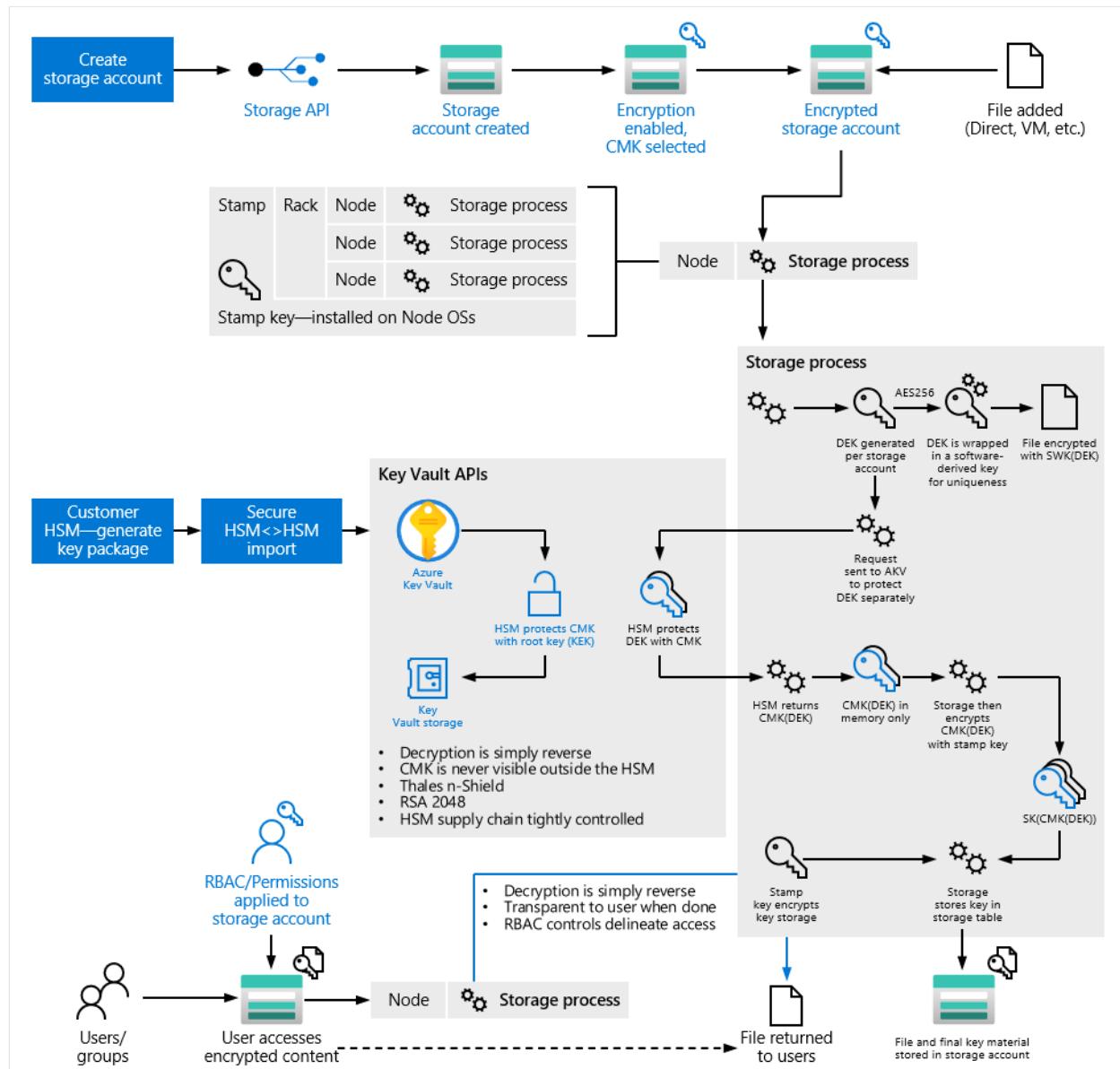


Figure 17. Encryption flow for Storage service encryption

Storage accounts are encrypted regardless of their performance tier (standard or premium) or deployment model (Azure Resource Manager or classic). All Azure Storage [redundancy options](#) support encryption and all copies of a storage account are

encrypted. All Azure Storage resources are encrypted, including blobs, disks, files, queues, and tables. All object metadata is also encrypted.

Because data encryption is performed by the Storage service, server-side encryption with CMK enables you to use any operating system types and images for your VMs. For your Windows and Linux IaaS VMs, Azure also provides Azure Disk encryption that enables you to encrypt managed disks with CMK within the Guest VM or EncryptionAtHost that encrypts disk data right at the host, as described in the next sections. Azure Storage service encryption also offers [double encryption of disk data at rest](#).

Azure Disk encryption

Azure Storage service encryption encrypts the page blobs that store Azure Virtual Machine disks. Moreover, you may optionally use [Azure Disk encryption](#) to encrypt Azure [Windows](#) and [Linux](#) IaaS Virtual Machine disks to increase storage isolation and assure cryptographic certainty of your data stored in Azure. This encryption includes [managed disks](#), as described later in this section. Azure disk encryption uses the industry standard [BitLocker](#) feature of Windows and the [DM-Crypt](#) feature of Linux to provide OS-based volume encryption that is integrated with Azure Key Vault.

Drive encryption through BitLocker and DM-Crypt is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers. BitLocker and DM-Crypt provide the most protection when used with a Trusted Platform Module (TPM) version 1.2 or higher. The TPM is a microcontroller designed to secure hardware through integrated cryptographic keys – it's commonly preinstalled on newer computers. BitLocker and DM-Crypt can use this technology to protect the keys used to encrypt disk volumes and provide integrity to computer boot process.

For managed disks, Azure Disk encryption allows you to encrypt the OS and Data disks used by an IaaS virtual machine; however, Data can't be encrypted without first encrypting the OS volume. The solution relies on Azure Key Vault to help you control and manage the disk encryption keys in key vaults. You can supply your own encryption keys, which are safeguarded in Azure Key Vault to support *bring your own key (BYOK)* scenarios, as described previously in [Data encryption key management](#) section.

Azure Disk encryption does not support Managed HSM or an on-premises key management service. Only key vaults managed by the Azure Key Vault service can be used to safeguard customer-managed encryption keys for Azure Disk encryption. See [Encryption at host](#) for other options involving Managed HSM.

ⓘ Note

Detailed instructions are available for creating and configuring a key vault for Azure Disk encryption with both [Windows](#) and [Linux](#) VMs.

Azure Disk encryption relies on two encryption keys for implementation, as described previously:

- *Data Encryption Key (DEK)* is a symmetric AES-256 key used to encrypt OS and Data volumes through BitLocker or DM-Crypt. DEK itself is encrypted and stored in an internal location close to the data.
- *Key Encryption Key (KEK)* is an asymmetric RSA-2048 key used to encrypt the Data Encryption Keys. KEK is kept in Azure Key Vault under your control including granting access permissions through Microsoft Entra ID.

The DEK, encrypted with the KEK, is stored separately and only an entity with access to the KEK can decrypt the DEK. Access to the KEK is guarded by Azure Key Vault where you can choose to store your keys in [FIPS 140 validated hardware security modules](#).

For [Windows VMs](#), Azure Disk encryption selects the encryption method in BitLocker based on the version of Windows, for example, XTS-AES 256 bit for Windows Server 2012 or greater. These crypto modules are FIPS 140 validated as part of the Microsoft [Windows FIPS validation program](#). For [Linux VMs](#), Azure Disk encryption uses the decrypt default of aes-xts-plain64 with a 256-bit volume master key that is FIPS 140 validated as part of DM-Crypt validation obtained by suppliers of Linux IaaS VM images in Microsoft Azure Marketplace.

Server-side encryption for managed disks

[Azure managed disks](#) are block-level storage volumes that are managed by Azure and used with Azure Windows and Linux virtual machines. They simplify disk management for Azure IaaS VMs by handling storage account management transparently for you. Azure managed disks automatically encrypt your data by default using [256-bit AES encryption](#) that is FIPS 140 validated. For encryption key management, you have the following choices:

- [Platform-managed keys](#) is the default choice that provides transparent data encryption at rest for managed disks whereby keys are managed by Microsoft.
- [Customer-managed keys](#) enables you to have control over your own keys that can be imported into or generated inside Azure Key Vault or Managed HSM. This approach relies on two sets of keys as described previously: DEK and KEK. DEK

encrypts the data using an AES-256 based encryption and is in turn encrypted by an RSA KEK that is stored in Azure Key Vault or Managed HSM.

Customer-managed keys (CMK) enable you to have [full control](#) over your encryption keys. You can grant access to managed disks in your Azure Key Vault so that your keys can be used for encrypting and decrypting the DEK. You can also disable your keys or revoke access to managed disks at any time. Finally, you have full audit control over key usage with Azure Key Vault monitoring to ensure that only managed disks or other authorized resources are accessing your encryption keys.

Encryption at host

Encryption at host works with server-side encryption to ensure data stored on the VM host is encrypted at rest and flows encrypted to the Storage service. The server hosting your VM encrypts your data with no performance impact or requirement for code running in your guest VM, and that encrypted data flows into Azure Storage using the keys configured for server-side encryption. For more information, see [Encryption at host - End-to-end encryption for your VM data](#). Encryption at host with CMK can use keys stored in Managed HSM or Key Vault, just like server-side encryption for managed disks.

You're [always in control of your customer data](#) in Azure. You can access, extract, and delete your customer data stored in Azure at will. When you terminate your Azure subscription, Microsoft takes the necessary steps to ensure that you continue to own your customer data. A common concern upon data deletion or subscription termination is whether another customer or Azure administrator can access your deleted data. The following sections explain how data deletion, retention, and destruction work in Azure.

Data deletion

Storage is allocated sparsely, which means that when a virtual disk is created, disk space isn't allocated for its entire capacity. Instead, a table is created that maps addresses on the virtual disk to areas on the physical disk and that table is initially empty. The first time you write data on the virtual disk, space on the physical disk is allocated and a pointer to it is placed in the table. For more information, see [Azure data security – data cleansing and leakage](#).

When you delete a blob or table entity, it will immediately get deleted from the index used to locate and access the data on the primary location, and then the deletion is done asynchronously at the geo-replicated copy of the data, if you provisioned [geo-redundant storage](#). At the primary location, you can immediately try to access the blob or entity, and you won't find it in your index, since Azure provides strong consistency for the delete. So, you can verify directly that the data has been deleted.

In Azure Storage, all disk writes are sequential. This approach minimizes the amount of disk “seeks” but requires updating the pointers to objects every time they’re written – new versions of pointers are also written sequentially. A side effect of this design is that it isn’t possible to ensure that a secret on disk is gone by overwriting it with other data. The original data will remain on the disk and the new value will be written sequentially. Pointers will be updated such that there’s no way to find the deleted value anymore. Once the disk is full, however, the system has to write new logs onto disk space that has been freed up by the deletion of old data. Instead of allocating log files directly from disk sectors, log files are created in a file system running NTFS. A background thread running on Azure Storage nodes frees up space by going through the oldest log file, copying blocks that are still referenced from that oldest log file to the current log file, and updating all pointers as it goes. It then deletes the oldest log file. Therefore, there are two categories of free disk space on the disk: (1) space that NTFS knows is free, where it allocates new log files from this pool; and (2) space within those log files that Azure Storage knows is free since there are no current pointers to it.

The sectors on the physical disk associated with the deleted data become immediately available for reuse and are overwritten when the corresponding storage block is reused for storing other data. The time to overwrite varies depending on disk utilization and activity. This process is consistent with the operation of a log-structured file system where all writes are written sequentially to disk. This process isn’t deterministic and there’s no guarantee when particular data will be gone from physical storage. **However, when exactly deleted data gets overwritten or the corresponding physical storage allocated to another customer is irrelevant for the key isolation assurance that no data can be recovered after deletion:**

- A customer can’t read deleted data of another customer.
- If anyone tries to read a region on a virtual disk that they haven’t yet written to, physical space won’t have been allocated for that region and therefore only zeroes would be returned.

Customers aren’t provided with direct access to the underlying physical storage. Since customer software only addresses virtual disks, there’s no way for another customer to express a request to read from or write to a physical address that is allocated to you or a physical address that is free.

Conceptually, this rationale applies regardless of the software that keeps track of reads and writes. For [Azure SQL Database](#), it’s the SQL Database software that does this enforcement. For Azure Storage, it’s the Azure Storage software. For nondurable drives of a VM, it’s the VHD handling code of the Host OS. The mapping from virtual to physical address takes place outside of the customer VM.

Finally, as described in [Data encryption at rest](#) section and depicted in Figure 16, the encryption key hierarchy relies on the Key Encryption Key (KEK) which can be kept in Azure Key Vault under your control (that is, customer-managed key – CMK) and used to encrypt the Data Encryption Key (DEK), which in turns encrypts data at rest using AES-256 symmetric encryption. Data in Azure Storage is encrypted at rest by default and you can choose to have encryption keys under your own control. In this manner, you can also prevent access to your data stored in Azure. Moreover, since the KEK is required to decrypt the DEKs, the KEK is effectively a single point by which DEK can be deleted via deletion of the KEK.

Data retention

During the term of your Azure subscription, you always have the ability to access, extract, and delete your data stored in Azure.

If your subscription expires or is terminated, Microsoft will preserve your customer data for a 90-day retention period to permit you to extract your data or renew your subscriptions. After this retention period, Microsoft will delete all your customer data within another 90 days, that is, your customer data will be permanently deleted 180 days after expiration or termination. Given the data retention procedure, you can control how long your data is stored by timing when you end the service with Microsoft. It's recommended that you don't terminate your service until you've extracted all data so that the initial 90-day retention period can act as a safety buffer should you later realize you missed something.

If you deleted an entire storage account by mistake, you should contact [Azure Support](#) for assistance with recovery. You can [create and manage support requests](#) in the Azure portal. A storage account deleted within a subscription is retained for two weeks to allow for recovery from accidental deletion, after which it's permanently deleted. However, when a storage object (for example, blob, file, queue, table) is itself deleted, the delete operation is immediate and irreversible. Unless you made a backup, deleted storage objects can't be recovered. For Blob storage, you can implement extra protection against accidental or erroneous modifications or deletions by enabling [soft delete](#). When [soft delete is enabled](#) for a storage account, blobs, blob versions, and snapshots in that storage account may be recovered after they're deleted, within a retention period that you specified. To avoid retention of data after storage account or subscription deletion, you can delete storage objects individually before deleting the storage account or subscription.

For accidental deletion involving Azure SQL Database, you should check backups that the service makes automatically and use point-in-time restore. For example, full database backup is done weekly, and differential database backups are done hourly.

Also, individual services (such as Azure DevOps) can have their own policies for [accidental data deletion](#).

Data destruction

If a disk drive used for storage suffers a hardware failure, it's securely [erased or destroyed](#) before decommissioning. The data on the drive is erased to ensure that the data can't be recovered by any means. When such devices are decommissioned, Microsoft follows the [NIST SP 800-88 R1](#) disposal process with data classification aligned to FIPS 199 Moderate. Magnetic, electronic, or optical media are purged or destroyed in accordance with the requirements established in NIST SP 800-88 R1 where the terms are defined as follows:

- **Purge** – “a media sanitization process that protects the confidentiality of information against a laboratory attack”, which involves “resources and knowledge to use nonstandard systems to conduct data recovery attempts on media outside their normal operating environment” using “signal processing equipment and specially trained personnel.” Note: For hard disk drives (including ATA, SCSI, SATA, SAS, and so on) a firmware-level secure-erase command (single-pass) is acceptable, or a software-level three-pass overwrite and verification (ones, zeros, random) of the entire physical media including recovery areas, if any. For solid state disks (SSD), a firmware-level secure-erase command is necessary.
- **Destroy** – “a variety of methods, including disintegration, incineration, pulverizing, shredding, and melting” after which the media “can't be reused as originally intended.”

Purge and Destroy operations must be performed using tools and processes approved by Microsoft Security. Records must be kept of the erasure and destruction of assets. Devices that fail to complete the Purge successfully must be degaussed (for magnetic media only) or destroyed.

In addition to technical implementation details that enable Azure compute, networking, and storage isolation, Microsoft has invested heavily in security assurance processes and practices to correctly develop logically isolated services and systems, as described in the next section.

Security assurance processes and practices

Azure isolation assurances are further enforced by Microsoft's internal use of the [Security Development Lifecycle](#) (SDL) and other strong security assurance processes to protect attack surfaces and mitigate threats. Microsoft has established industry-

leading processes and tooling that provides high confidence in the Azure isolation guarantee.

- **Security Development Lifecycle (SDL)** – The Microsoft SDL introduces security and privacy considerations throughout all phases of the development process, helping developers build highly secure software, address security compliance requirements, and reduce development costs. The guidance, best practices, [tools](#), and processes in the Microsoft SDL are [practices](#) used internally to build all Azure services and create more secure products and services. This process is also publicly documented to share Microsoft's learnings with the broader industry and incorporate industry feedback to create a stronger security development process.
- **Tooling and processes** – All Azure code is subject to an extensive set of both static and dynamic analysis tools that identify potential vulnerabilities, ineffective security patterns, memory corruption, user privilege issues, and other critical security problems.
 - *Purpose built fuzzing* – A testing technique used to find security vulnerabilities in software products and services. It consists of repeatedly feeding modified, or fuzzed, data to software inputs to trigger hangs, exceptions, and crashes, which are fault conditions that could be used by an attacker to disrupt or take control of applications and services. The Microsoft SDL recommends [fuzzing](#) all attack surfaces of a software product, especially those surfaces that expose a data parser to untrusted data.
 - *Live-site penetration testing* – Microsoft conducts [ongoing live-site penetration testing](#) to improve cloud security controls and processes, as part of the Red Teaming program described later in this section. Penetration testing is a security analysis of a software system performed by skilled security professionals simulating the actions of a hacker. The objective of a penetration test is to uncover potential vulnerabilities resulting from coding errors, system configuration faults, or other operational deployment weaknesses. The tests are conducted against Azure infrastructure and platforms and Microsoft's own tenants, applications, and data. Your tenants, applications, and data hosted in Azure are never targeted; however, you can conduct [your own penetration testing](#) of your applications deployed in Azure.
 - *Threat modeling* – A core element of the Microsoft SDL. It's an engineering technique used to help identify threats, attacks, vulnerabilities, and countermeasures that could affect applications and services. [Threat modeling](#) is part of the Azure routine development lifecycle.
 - *Automated build alerting of changes to attack surface area* – [Attack Surface Analyzer](#) is a Microsoft-developed open-source security tool that analyzes the attack surface of a target system and reports on potential security vulnerabilities

introduced during the installation of software or system misconfiguration. The core feature of Attack Surface Analyzer is the ability to “diff” an operating system’s security configuration, before and after a software component is installed. This feature is important because most installation processes require elevated privileges, and once granted, they can lead to unintended system configuration changes.

- **Mandatory security training** – The Microsoft Azure security training and awareness program requires all personnel responsible for Azure development and operations to take essential training and any extra training based on individual job requirements. These procedures provide a standard approach, tools, and techniques used to implement and sustain the awareness program. Microsoft has implemented a security awareness program called STRIKE that provides monthly e-mail communication to all Azure engineering personnel about security awareness and allows employees to register for in-person or online security awareness training. STRIKE offers a series of security training events throughout the year plus STRIKE Central, which is a centralized online resource for security awareness, training, documentation, and community engagement.
- **Bug Bounty Program** – Microsoft strongly believes that close partnership with academic and industry researchers drives a higher level of security assurance for you and your data. Security researchers play an integral role in the Azure ecosystem by discovering vulnerabilities missed in the software development process. The [Microsoft Bug Bounty Program](#) is designed to supplement and encourage research in relevant technologies (for example, encryption, spoofing, hypervisor isolation, elevation of privileges, and so on) to better protect Azure’s infrastructure and your data. As an example, for each critical vulnerability identified in the Azure Hypervisor, Microsoft compensates security researchers up to \$250,000 – a significant amount to incentivize participation and vulnerability disclosure. The bounty range for [vulnerability reports on Azure services](#) is up to \$60,000.
- **Red Team activities** – Microsoft uses [Red Teaming](#), a form of live site penetration testing against Microsoft-managed infrastructure, services, and applications. Microsoft simulates real-world breaches, continuously monitors security, and practices security incident response to test and improve Azure security. Red Teaming is predicated on the Assume Breach security strategy and executed by two core groups: Red Team (attackers) and Blue Team (defenders). The approach is designed to test Azure systems and operations using the same tactics, techniques, and procedures as real adversaries against live production infrastructure, without the foreknowledge of the infrastructure and platform Engineering or Operations teams. This approach tests security detection and response capabilities, and helps identify production vulnerabilities, configuration errors, invalid assumptions, or

other security issues in a controlled manner. Every Red Team breach is followed by full disclosure between the Red Team and Blue Team to identify gaps, address findings, and significantly improve breach response.

If you're accustomed to a traditional on-premises data center deployment, you would typically conduct a risk assessment to gauge your threat exposure and formulate mitigating measures when migrating to the cloud. In many of these instances, security considerations for traditional on-premises deployment tend to be well understood whereas the corresponding cloud options tend to be new. The next section is intended to help you with this comparison.

Logical isolation considerations

A multi-tenant cloud platform implies that multiple customer applications and data are stored on the same physical hardware. Azure uses [logical isolation](#) to segregate your applications and data from other customers. This approach provides the scale and economic benefits of multi-tenant cloud services while rigorously helping enforce controls designed to keep other customers from accessing your data or applications. If you're migrating from traditional on-premises physically isolated infrastructure to the cloud, this section addresses concerns that may be of interest to you.

Physical versus logical security considerations

Table 6 provides a summary of key security considerations for physically isolated on-premises deployments (bare metal) versus logically isolated cloud-based deployments (Azure). It's useful to review these considerations prior to examining risks identified to be specific to shared cloud environments.

Table 6. Key security considerations for physical versus logical isolation

Expand table

Security consideration	On-premises	Azure
Firewalls, networking	<ul style="list-style-type: none">- Physical network enforcement (switches, and so on)- Physical host-based firewall can be manipulated by compromised application- two layers of enforcement	<ul style="list-style-type: none">- Physical network enforcement (switches, and so on)- Hyper-V host virtual network switch enforcement can't be changed from inside VM- VM host-based firewall can be manipulated by compromised

Security consideration	On-premises	Azure
		application - three layers of enforcement
Attack surface area	- Large hardware attack surface exposed to complex workloads, enables firmware based advanced persistent threat (APT)	- Hardware not directly exposed to VM, no potential for APT to persist in firmware from VM - Small software-based Hyper-V attack surface area with low historical bug counts exposed to VM
Side channel attacks	- Side channel attacks may be a factor, although reduced vs. shared hardware	- Side channel attacks assume control over VM placement across applications; may not be practical in large cloud service
Patching	- Varied effective patching policy applied across host systems - Highly varied/fragile updating for hardware and firmware	- Uniform patching policy applied across host and VMs
Security analytics	- Security analytics dependent on host-based security solutions, which assume host/security software hasn't been compromised	- Outside VM (hypervisor based) forensics/snapshot capability allows assessment of potentially compromised workloads
Security policy	- Security policy verification (patch scanning, vulnerability scanning, and so on) subject to tampering by compromised host - Inconsistent security policy applied across customer entities	- Outside VM verification of security policies - Possible to enforce uniform security policies across customer entities
Logging and monitoring	- Varied logging and security analytics solutions	- Common Azure platform logging and security analytics solutions - Most existing on-premises / varied logging and security analytics solutions also work
Malicious insider	- Persistent threat caused by system admins having elevated access rights typically for duration of employment	- Greatly reduced threat because admins have no default access rights

Listed below are key risks that are unique to shared cloud environments that may need to be addressed when accommodating sensitive data and workloads.

Exploitation of vulnerabilities in virtualization technologies

Compared to traditional on-premises hosted systems, Azure provides a greatly **reduced attack surface** by using a locked-down Windows Server core for the Host OS layered over the Hypervisor. Moreover, by default, guest PaaS VMs don't have any user accounts to accept incoming remote connections and the default Windows administrator account is disabled. Your software in PaaS VMs is restricted by default to running under a low-privilege account, which helps protect your service from attacks by its own end users. You can modify these permissions, and you can also choose to configure your VMs to allow remote administrative access.

PaaS VMs offer more advanced **protection against persistent malware** infections than traditional physical server solutions, which if compromised by an attacker can be difficult to clean, even after the vulnerability is corrected. The attacker may have left behind modifications to the system that allow re-entry, and it's a challenge to find all such changes. In the extreme case, the system must be reimaged from scratch with all software reinstalled, sometimes resulting in the loss of application data. With PaaS VMs, reimaging is a routine part of operations, and it can help clean out intrusions that haven't even been detected. This approach makes it more difficult for a compromise to persist.

Side channel attacks

Microsoft has been at the forefront of mitigating **speculative execution side channel attacks** that exploit hardware vulnerabilities in modern processors that use hyper-threading. In many ways, these issues are similar to the Spectre (variant 2) side channel attack, which was disclosed in 2018. Multiple new speculative execution side channel issues were disclosed by both Intel and AMD in 2022. To address these vulnerabilities, Microsoft has developed and optimized Hyper-V [HyperClear](#), a comprehensive and high performing side channel vulnerability mitigation architecture. HyperClear relies on three main components to ensure strong inter-VM isolation:

- **Core scheduler** to avoid sharing of a CPU core's private buffers and other resources.
- **Virtual-processor address space isolation** to avoid speculative access to another virtual machine's memory or another virtual CPU core's private state.
- **Sensitive data scrubbing** to avoid leaving private data anywhere in hypervisor memory other than within a virtual processor's private address space so that this data can't be speculatively accessed in the future.

These protections have been deployed to Azure and are available in Windows Server 2016 and later supported releases.

 **Note**

The Hyper-V HyperClear architecture has proven to be a readily extensible design that helps provide strong isolation boundaries against a variety of speculative execution side channel attacks with negligible impact on performance.

When VMs belonging to different customers are running on the same physical server, it's the Hypervisor's job to ensure that they can't learn anything important about what the other customer's VMs are doing. Azure helps block unauthorized direct communication by design; however, there are subtle effects where one customer might be able to characterize the work being done by another customer. The most important of these effects are timing effects when different VMs are competing for the same resources. By carefully comparing operations counts on CPUs with elapsed time, a VM can learn something about what other VMs on the same server are doing. These exploits have received plenty of attention in the academic press where researchers have been seeking to learn more specific information about what's going on in a peer VM.

Of particular interest are efforts to learn the **cryptographic keys of a peer VM** by measuring the timing of certain memory accesses and inferring which cache lines the victim's VM is reading and updating. Under controlled conditions with VMs using hyper-threading, successful attacks have been demonstrated against commercially available implementations of cryptographic algorithms. In addition to the previously mentioned Hyper-V HyperClear mitigation architecture that's in use by Azure, there are several extra mitigations in Azure that reduce the risk of such an attack:

- The standard Azure cryptographic libraries have been designed to resist such attacks by not having cache access patterns depend on the cryptographic keys being used.
- Azure uses an advanced VM host placement algorithm that is highly sophisticated and nearly impossible to predict, which helps reduce the chances of adversary-controlled VM being placed on the same host as the target VM.
- All Azure servers have at least eight physical cores and some have many more. Increasing the number of cores that share the load placed by various VMs adds noise to an already weak signal.
- You can provision VMs on hardware dedicated to a single customer by using [Azure Dedicated Host](#) or [Isolated VMs](#), as described in [Physical isolation](#) section. However, physical tenant isolation increases deployment cost and may not be

required in most scenarios given the strong logical isolation assurances provided by Azure.

Overall, PaaS – or any workload that autocreates VMs – contributes to churn in VM placement that leads to randomized VM allocation. Random placement of your VMs makes it much harder for attackers to get on the same host. In addition, host access is hardened with greatly reduced attack surface that makes these types of exploits difficult to sustain.

Summary

A multi-tenant cloud platform implies that multiple customer applications and data are stored on the same physical hardware. Azure uses logical isolation to segregate your applications and data from other customers. This approach provides the scale and economic benefits of multi-tenant cloud services while rigorously helping prevent other customers from accessing your data or applications.

Azure addresses the perceived risk of resource sharing by providing a trustworthy foundation for assuring multi-tenant, cryptographically certain, logically isolated cloud services using a common set of principles:

- User access controls with authentication and identity separation that uses Microsoft Entra ID and Azure role-based access control (Azure RBAC).
- Compute isolation for processing, including both logical and physical compute isolation.
- Networking isolation including separation of network traffic and data encryption in transit.
- Storage isolation with data encryption at rest using advanced algorithms with multiple ciphers and encryption keys and provisions for customer-managed keys (CMK) under your control in Azure Key Vault.
- Security assurance processes embedded in service design to correctly develop logically isolated services, including Security Development Lifecycle (SDL) and other strong security assurance processes to protect attack surfaces and mitigate risks.

In line with the shared responsibility model in cloud computing, this article provides you with guidance for activities that are part of your responsibility. It also explores design principles and technologies available in Azure to help you achieve your secure isolation objectives.

Next steps

Learn more about:

- [Azure security fundamentals documentation](#)
- [Azure infrastructure security](#)
- [Azure platform integrity and security](#)
- [Azure Government overview](#)
- [Azure Government security](#)
- [Azure Government compliance](#)
- [Azure and other Microsoft services compliance offerings](#)

Secure Azure Computing Architecture (SACA)

Article • 10/03/2022

US Department of Defense (DoD) customers who deploy workloads to Azure have asked for guidance to set up secure virtual networks and configure the security tools and services that are stipulated by DoD standards and practice.

In 2017, the Defense Information System Agency (DISA) published the [Secure Cloud Computing Architecture \(SCCA\) Functional Requirements Document \(FRD\)](#) . SCCA describes the functional objectives for securing the Defense Information System Network's (DISN) and commercial cloud provider connection points. SCCA also describes how mission owners secure cloud applications at the connection boundary. Every DoD entity that connects to the commercial cloud must follow the guidelines set forth in the SCCA FRD.

The SCCA has four components:

- Boundary Cloud Access Point (BCAP)
- Virtual Datacenter Security Stack (VDSS)
- Virtual Datacenter Managed Services (VDMS)
- Trusted Cloud Credential Manager (TCCM)

Microsoft has developed a solution that helps you meet the SCCA requirements for both [DoD IL4](#) and [DoD IL5](#) workloads that run in Azure. This Azure-specific solution is called the **Secure Azure Computing Architecture (SACA)**, and it can help you comply with the SCCA FRD. It can enable you to move workloads into Azure after you're connected.

SCCA guidance and architectures are specific to DoD customers, but they also help civilian customers comply with [Trusted Internet Connections \(TIC\)](#) guidance and help commercial customers that want to implement a secure DMZ to protect their Azure environments.

Secure Cloud Computing Architecture components

Boundary Cloud Access Point (BCAP)

The purpose of the BCAP is to protect the DISN from attacks that originate in the cloud environment. BCAP performs intrusion detection and prevention. It also filters out unauthorized traffic. This component can be colocated with other components of the SCCA. We recommend that you deploy this component by using physical hardware. BCAP security requirements are listed in the following table.

BCAP security requirements

Req. ID	BCAP Security Requirements
2.1.1.1.1	The BCAP shall provide the capability to detect and prevent malicious code injection into the DISN originating from the CSE
2.1.1.1.2	The BCAP shall provide the capability to detect and thwart single and multiple node DOS attacks
2.1.1.1.3	The BCAP shall provide the ability to perform detection and prevention of traffic flow having unauthorized source and destination IP addresses, protocols, and Transmission Control Protocol (TCP)/User Datagram Protocol (UDP) ports
2.1.1.1.4	The BCAP shall provide the capability to detect and prevent IP Address Spoofing and IP Route Hijacking
2.1.1.1.5	The BCAP shall provide the capability to prevent device identity policy infringement (prevent rogue device access)
2.1.1.1.6	The BCAP shall provide the capability to detect and prevent passive and active network enumeration scanning originating from within the CSE
2.1.1.1.7	The BCAP shall provide the capability to detect and prevent unauthorized data exfiltration from the DISN to an endpoint inside CSE
2.1.1.1.8	The BCAP and/or BCAP Management System shall provide the capability to sense, correlate, and warn on advanced persistent threats
2.1.1.1.9	The BCAP shall provide the capability to detect custom traffic and activity signatures
2.1.1.1.10	The BCAP shall provide an interface to conduct ports, protocols, and service management (PPSM) activities in order to provide control for BCND provider
2.1.1.1.11	The BCAP shall provide full packet capture (FPC) for traversing communications
2.1.1.1.12	The BCAP shall provide network packet flow metrics and statistics for all traversing communications
2.1.1.1.13	The BCAP shall provide the capability to detect and prevent application session hijacking

Virtual Datacenter Security Stack (VDSS)

The purpose of the VDSS is to protect DoD mission-owner applications that are hosted in Azure. VDSS performs the bulk of the security operations in the SCCA. It conducts traffic inspection to secure the applications that run in Azure. This component can be provided within your Azure environment.

VDSS security requirements

Req. ID	VDSS Security Requirements
2.1.2.1	The VDSS shall maintain virtual separation of all management, user, and data traffic
2.1.2.2	The VDSS shall allow the use of encryption for segmentation of management traffic.
2.1.2.3	The VDSS shall provide a reverse proxy capability to handle access requests from client systems
2.1.2.4	The VDSS shall provide a capability to inspect and filter application layer conversations based on a predefined set of rules (including HTTP) to identify and block malicious content
2.1.2.5	The VDSS shall provide a capability that can distinguish and block unauthorized application layer traffic
2.1.2.6	The VDSS shall provide a capability that monitors network and system activities to detect and report malicious activities for traffic entering and exiting Mission Owner virtual private networks/enclaves
2.1.2.7	The VDSS shall provide a capability that monitors network and system activities to stop or block detected malicious activity
2.1.2.8	The VDSS shall inspect and filter traffic traversing between mission owner virtual private networks/enclaves.
2.1.2.9	The VDSS shall perform break and inspection of SSL/TLS communication traffic supporting single and dual authentication for traffic destined to systems hosted within the CSE12.
2.1.2.10	The VDSS shall provide an interface to conduct ports, protocols, and service management (PPSM) activities in order to provide control for MCD operators
2.1.2.11	The VDSS shall provide a monitoring capability that captures log files and event data for cybersecurity analysis
2.1.2.12	The VDSS shall provide or feed security information and event data to an allocated archiving system for common collection, storage, and access to event logs by privileged users performing Boundary and Mission CND activities
2.1.2.13	The VDSS shall provide a FIPS-140-2 compliant encryption key management system for storage of DoD generated and assigned server private encryption key credentials for access and use by the Web Application Firewall (WAF) in the execution of SSL/TLS break and inspection of encrypted communication sessions.
2.1.2.14	The VDSS shall provide the capability to detect and identify application session hijacking
2.1.2.15	The VDSS shall provide a DoD DMZ Extension to support to support Internet Facing Applications (IFAs)
2.1.2.16	The VDSS shall provide full packet capture (FPC) or cloud service equivalent FPC capability for recording and interpreting traversing communication
2.1.2.17	The VDSS shall provide network packet flow metrics and statistics for all traversing communications
2.1.2.18	The VDSS shall provide for the inspection of traffic entering and exiting each mission owner virtual private network.

Virtual Datacenter Managed Services (VDMS)

The purpose of VDMS is to provide host security and shared data center services. The functions of VDMS can either run in the hub of your SCCA or the mission owner can deploy pieces of it in their own Azure subscription. This component can be provided within your Azure environment.

VDMS security requirements

Req. ID	VDMS Security Requirements
2.1.3.1	The VDMS shall provide Assured Compliance Assessment Solution (ACAS), or approved equivalent, to conduct continuous monitoring for all enclaves within the CSE
2.1.3.2	The VDMS shall provide Host Based Security System (HBSS), or approved equivalent, to manage endpoint security for all enclaves within the CSE
2.1.3.3	The VDMS shall provide identity services to include an Online Certificate Status Protocol (OCSP) responder for remote system DoD Common Access Card (CAC) two-factor authentication of DoD privileged users to systems instantiated within the CSE
2.1.3.4	The VDMS shall provide a configuration and update management system to serve systems and applications for all enclaves within the CSE
2.1.3.5	The VDMS shall provide logical domain services to include directory access, directory federation, Dynamic Host Configuration Protocol (DHCP), and Domain Name System (DNS) for all enclaves within the CSE
2.1.3.6	The VDMS shall provide a network for managing systems and applications within the CSE that is logically separate from the user and data networks
2.1.3.7	The VDMS shall provide a system, security, application, and user activity event logging and archiving system for common collection, storage, and access to event logs by privileged users performing BCP and MCP activities.
2.1.3.8	The VDMS shall provide for the exchange of DoD privileged user authentication and authorization attributes with the CSP's Identity and access management system to enable cloud system provisioning, deployment, and configuration
2.1.3.9	The VDMS shall implement the technical capabilities necessary to execute the mission and objectives of the TCCM role.

Trusted Cloud Credential Manager (TCCM)

TCCM is a business role. This individual is responsible for managing the SCCA. Their duties are to:

- Establish plans and policies for account access to the cloud environment.
- Ensure that identity and access management is operating properly.
- Maintain the Cloud Credential Management Plan.

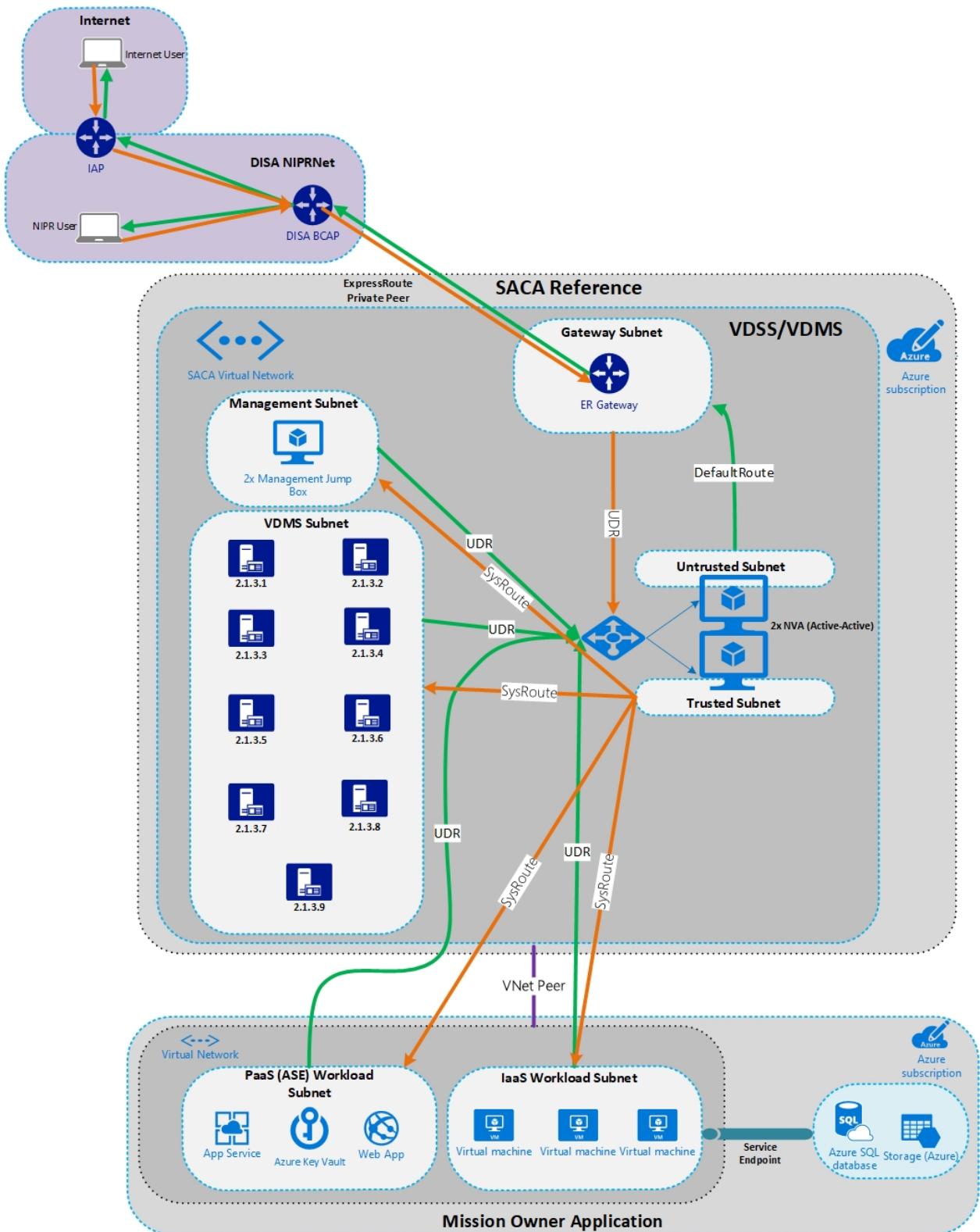
This individual is appointed by the authorizing official. The BCAP, VDSS, and VDMS provide the capabilities that the TCCM needs to perform their job.

TCCM security requirements

Req. ID	TCCM Security Requirements
2.1.4.1	The TCCM shall develop and maintain a Cloud Credential Management Plan (CCMP) to address the implementation of policies, plans, and procedures that will be applied to mission owner customer portal account credential management
2.1.4.2	The TCCM shall collect, audit, and archive all Customer Portal activity logs and alerts
2.1.4.3	The TCCM shall ensure activity log alerts are shared with, forwarded to, or retrievable by DoD privileged users engaged in MCP and BCP activities
2.1.4.4	The TCCM shall, as necessary for information sharing, create log repository access accounts for access to activity log data by privileged users performing both MCP and BCP activities
2.1.4.5	The TCCM shall recover and securely control customer portal account credentials prior to mission application connectivity to the DISN
2.1.4.6	The TCCM shall create, issue, and revoke, as necessary, role-based access least privileged customer portal credentials to mission owner application and system administrators (i.e., DoD privileged users).
2.1.4.7	The TCCM shall limit, to the greatest extent possible, the issuance of customer portal and other CSP service (e.g., API, CLI) end-point privileges to configure network, application, and CSO elements
2.1.4.8	The TCCM shall ensure that privileged users are not allowed to use CSP IdAM derived credentials which possess the ability to unilaterally create unauthorized network connections within the CSE, between the CSO and the CSP's private network, or to the Internet

SACA components and planning considerations

The SACA reference architecture is designed to deploy the VDSS and VDMS components in Azure and to enable the TCCM. This architecture is modular. All the pieces of VDSS and VDMS can live in a centralized hub or in multiple virtual networks. Some of the controls can be met in the mission owner space or even on premises. The following diagram shows this architecture:



When you plan your SCCA compliance strategy and technical architecture, consider the following topics from the beginning because they affect every customer. The following issues have come up with DoD customers and tend to slow down planning and execution.

Which BCAP will your organization use?

- DISA BCAP:

- DISA has two Gen 2 BCAPs that they currently operate and maintain, with three new Gen 3 BCAPs coming online soon.
- DISA's BCAPs all have Azure ExpressRoute circuits to Azure, which can be used by Government and DoD customers for connectivity.
- DISA has an enterprise-level Microsoft peering session for customers who want to subscribe to Microsoft software as a service (SaaS) tools, such as Microsoft 365. By using the DISA BCAP, you can enable connectivity and peering to your SACA instance.
- We recommend that you use the DISA BCAP. This option is readily available, has built-in redundancy, and has customers that operate on it today in production.
- Build your own BCAP:
 - This option requires you to lease space in a colocated data center and set up an ExpressRoute circuit to Azure.
 - This option requires additional approval from the DoD CIO.
 - Because of the additional approval and a physical build-out, this option takes the most time, and is difficult to attain.
- DoD routable IP space:
 - You must use DoD routable IP space at your edge. The option to use NAT to connect those spaces to private IP space in Azure is available.
 - Contact the DoD Network Information Center (NIC) to obtain IP space. You need it as part of your System/Network Approval Process (SNAP) submission with DISA.
 - If you plan to use NAT to connect private address space in Azure, you need a minimum of a /24 subnet of address space assigned from the NIC for each region where you plan to deploy SACA.
- Redundancy:
 - Deploy a SACA instance to at least two regions for failover capabilities.
 - Connect to at least two BCAPs via separate ExpressRoute circuits. Both ExpressRoute connections can then be linked to each region's SACA instance.
- DoD component-specific requirements:
 - Does your organization have any specific requirements outside the SCCA requirements? Some organizations have specific IPS requirements.
- SACA is a modular architecture:
 - Use only the components you need for your environment.
 - Deploy network virtual appliances in a single tier or multi-tier.
 - Use cloud-native IPS or bring-your-own IPS.

Which automated solution will you use to deploy VDSS?

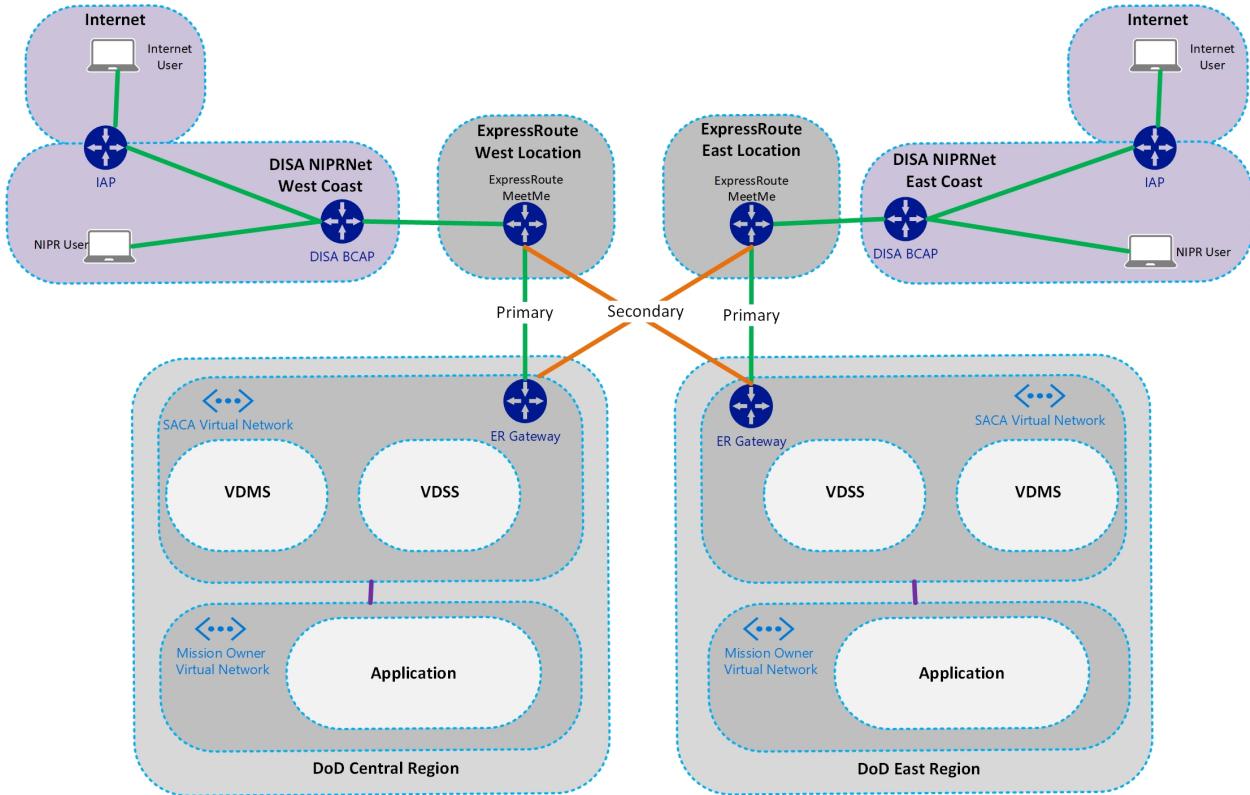
As mentioned earlier, you can build the SACA reference by using a variety of appliances and Azure services. Microsoft has automated solution templates to deploy the SACA with native services or with solutions from partners like Palo Alto Networks, F5, and Citrix. These solutions are covered in the following section.

Which Azure services will you use?

- There are Azure services that can meet requirements for log analytics, host-based protection, and IDS functionality. It's possible that some services aren't generally available in Microsoft Azure DoD regions. In this case, you might need to use third-party tools if these Azure services can't meet your requirements. Look at the tools you're comfortable with and the feasibility of using Azure native tooling.
- We recommend that you use as many Azure native tools as possible. They're built with cloud security in mind and seamlessly integrate with the rest of the Azure platform. Use the Azure native tools in the following list to meet various SCCA requirements:
 - [Azure Monitor](#)
 - [Microsoft Defender for Cloud](#)
 - [Network Watcher](#)
 - [Azure Key Vault](#)
 - [Microsoft Entra ID](#)
 - [Application Gateway](#)
 - [Azure Firewall](#)
 - [Azure Front Door](#)
 - [Network security groups](#)
 - [Azure DDoS Protection](#)
 - [Microsoft Sentinel](#)
- Sizing
 - A sizing exercise must be completed. Look at the number of concurrent connections you might have through the SACA instance and the network throughput requirements.
 - This step is critical. It helps to size the VMs, ExpressRoute circuits, and identify the licenses that are required from the various vendors you use in your SACA deployment.
 - A good cost analysis can't be done without the sizing exercise. Correct sizing also allows for best performance.

Most common deployment scenario

Several Microsoft customers have gone through the full deployment or at least the planning stages of their SACA environments. Their experiences revealed insight into the most common deployment scenario. The following diagram shows the most common architecture:



As you can see from the diagram, customers typically subscribe to two of the DISA BCAPs. An ExpressRoute private peer is enabled to Azure at each DISA BCAP location. These ExpressRoute peers are then linked to the virtual network gateway in each Azure region. All ingress and egress traffic flows through SACA, via the ExpressRoute connection to the DISA BCAP.

Mission owners then choose the Azure regions in which they plan to deploy their applications. They use virtual network peering to connect their application's virtual network to the SACA virtual network. Then they force tunnel all their traffic through the VDSS instance.

We recommend this architecture because it meets SCCA requirements. It's highly available, scales easily, and simplifies deployment and management.

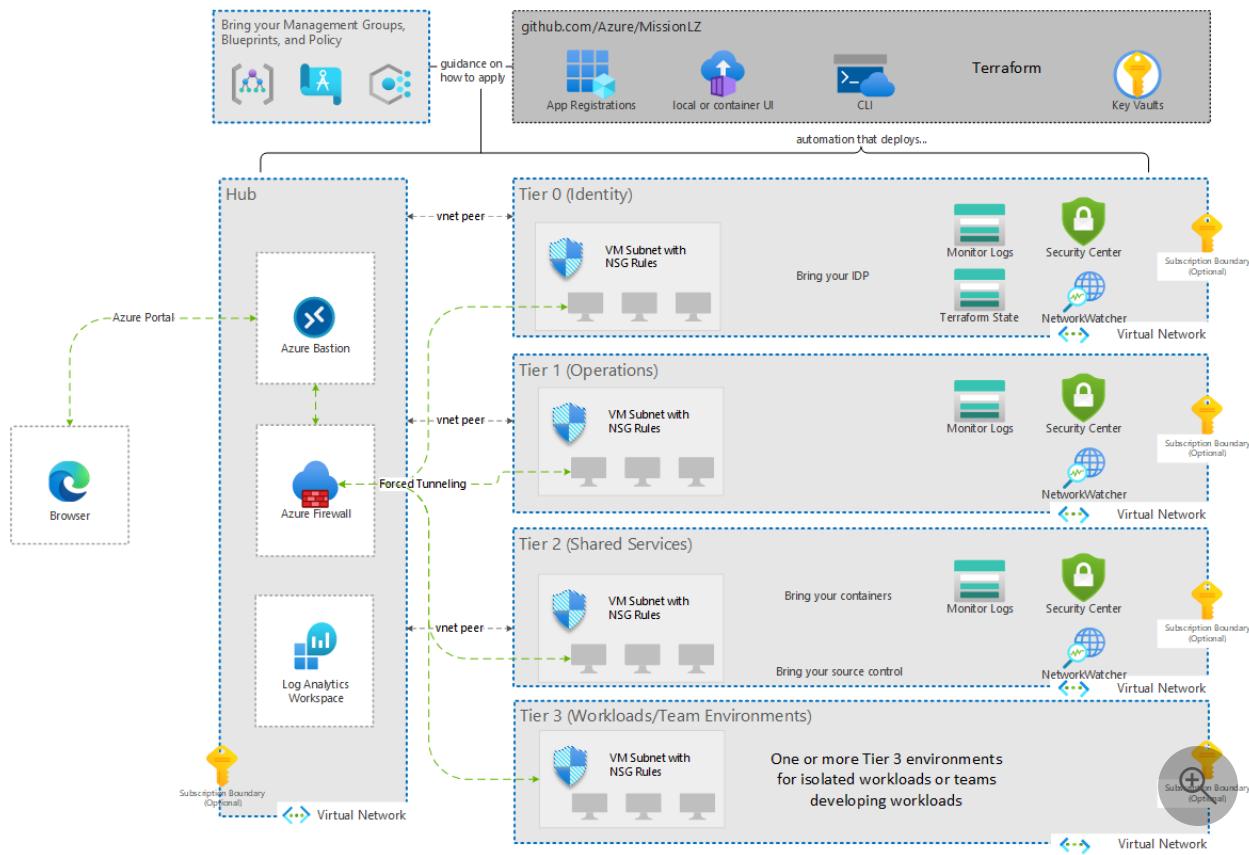
Automated SACA deployment options

As mentioned previously, Microsoft has partnered with vendors to create automated SACA infrastructure templates. These templates deploy the following Azure components:

- SACA virtual network
 - VDMS subnet
 - This subnet is where VMs and services used for VDMS are deployed, including the jump box VMs.
 - Untrusted, trusted, management, or AzureFirewallSubnet subnets
 - These subnets are where virtual appliances or Azure Firewall are deployed.
- Management jump box virtual machines
 - They're used for out-of-band management of the environment.
- Network virtual appliances
- Azure Bastion
 - Bastion is used to securely connect to VMs over SSL
- Public IPs
 - They're used for the front end until ExpressRoute is brought online. These IPs translate to the back-end Azure private address space.
- Route tables
 - Applied during automation, these route tables force tunnel all traffic through the virtual appliance via the internal load balancer.
- Azure load balancers - Standard SKU
 - They're used to load-balance traffic across the third-party appliances.
- Network security groups
 - They're used to control which types of traffic can traverse to certain endpoints.

Azure SACA deployment

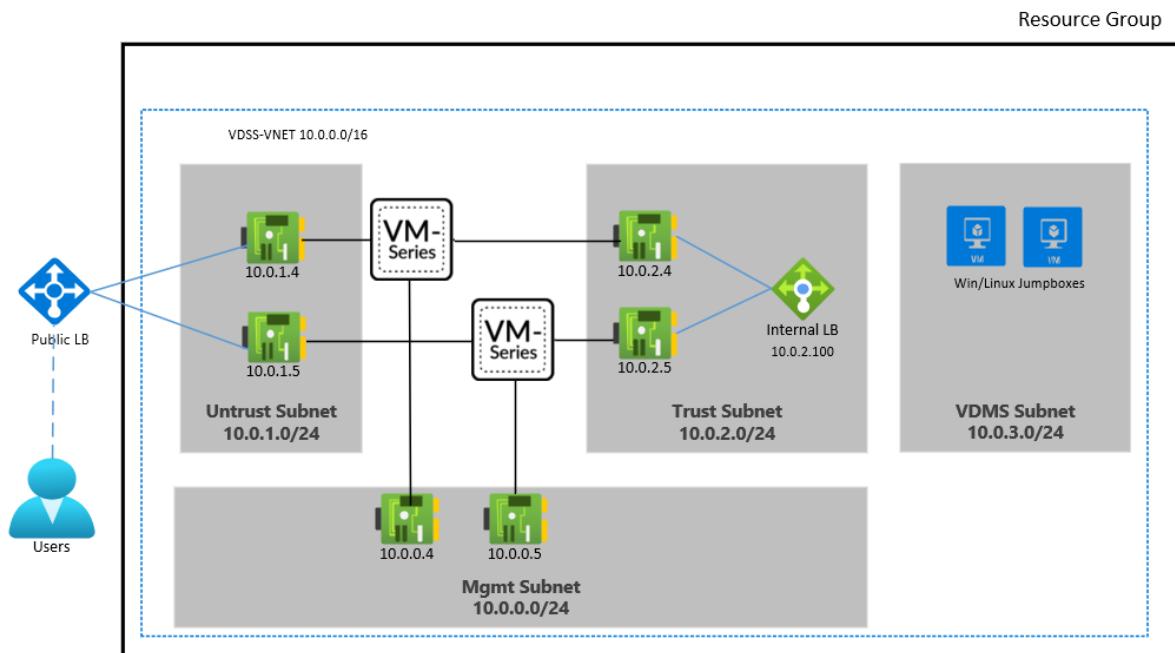
You can use the Mission Landing Zone deployment template to deploy into one or multiple subscriptions, depending on the requirements of your environment. It uses built-in Azure services that have no dependencies on third-party licenses. The template uses Azure Firewall and other security services to deploy an architecture that is SCCA-compliant.



For the Azure documentation and deployment scripts, see [Mission Landing Zone](#) ↗.

Palo Alto Networks SACA deployment

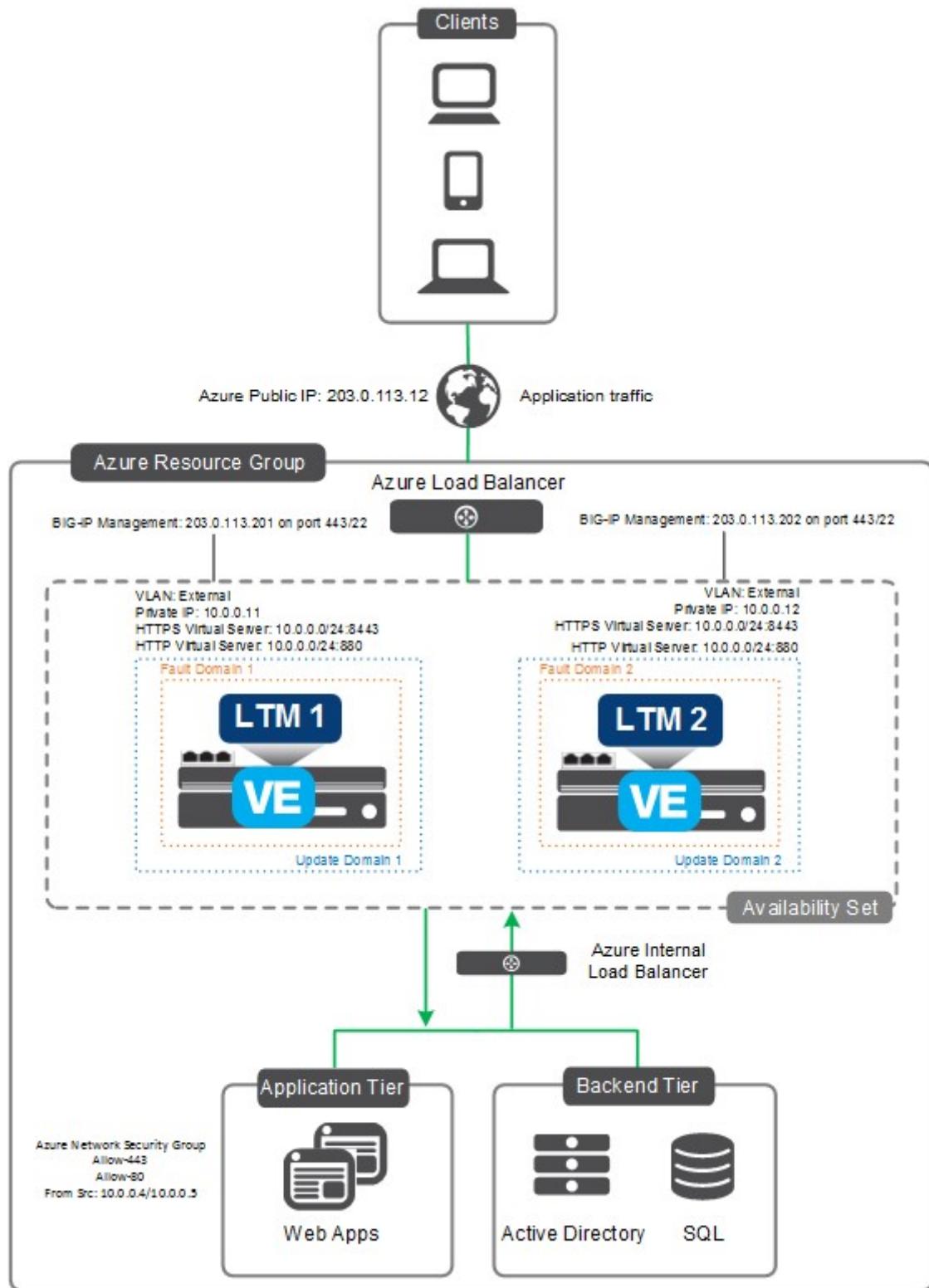
The Palo Alto Networks deployment template deploys one to many VM-Series appliances, as well as the VDMS staging and routing to enable a one-tier, VDSS-compliant architecture. This architecture meets the SACA requirements.



For the Palo Alto Networks documentation and deployment script, see [SACA implementation for Palo Alto Networks on Azure](#).

F5 Networks SACA deployment

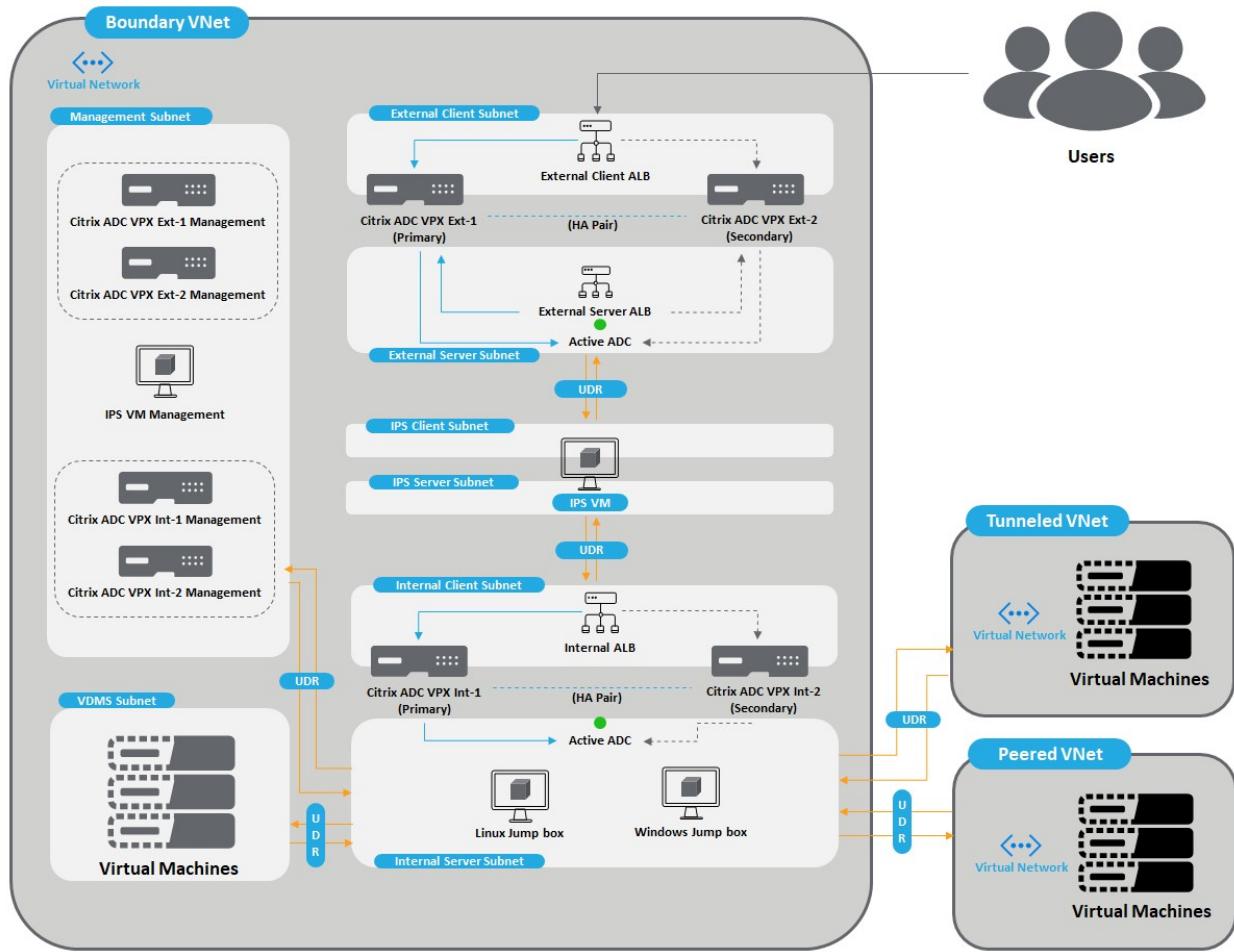
Two separate F5 deployment templates cover two different architectures. The first template has only one layer of F5 appliances in an active-active highly available configuration. This architecture meets the SCCA requirements. The second template adds a second layer of active-active highly available F5s. This second layer allows you to add your own IPS separate from F5 in between the F5 layers. Not all DoD components have specific IPS prescribed for use. If that's the case, the single layer of F5 appliances works for most because that architecture includes IPS on the F5 devices.



For the F5 documentation and deployment script, see [F5 and Azure SACA](#).

Citrix SACA deployment

A Citrix deployment template deploys two layers of highly available Citrix ADC appliances. This architecture meets the VDSS requirements.



For the Citrix documentation and deployment script, see [SACA based deployment](#).

Next steps

- Acquiring and accessing Azure Government
- Azure Government overview
- Azure Government security
- Azure Government compliance
- Trusted Internet Connections (TIC) with Azure
- Azure guidance for secure isolation
- FedRAMP High
- DoD Impact Level 4
- DoD Impact Level 5
- DoD Impact Level 6
- Azure and other Microsoft cloud services compliance scope
- Azure Policy overview
- Azure Policy regulatory compliance built-in initiatives
- Security control mapping with Azure landing zones

Planning identity for Azure Government applications

Article • 10/12/2023

Microsoft Azure Government provides the same ways to build applications and manage identities as Azure Public. Azure Government customers may already have a Microsoft Entra Public tenant or may create a tenant in Microsoft Entra Government. This article provides guidance on identity decisions based on the application and location of your identity.

Identity models

Before determining the identity approach for your application, you need to know what identity types are available to you. There are three types: On-premises identity, Cloud identity, and Hybrid identity.

On-premises identity	Cloud identity	Hybrid identity
On-premises identities belong to on-premises Active Directory environments that most customers use today.	Cloud identities originate, exist only, and are managed in Microsoft Entra ID.	Hybrid identities originate as on-premises identities, but become hybrid through directory synchronization to Microsoft Entra ID. After directory synchronization, they exist both on-premises and in the cloud, hence hybrid.

ⓘ Note

Hybrid comes with deployment options (synchronized identity, federated identity, and so on) that all rely on directory synchronization and mostly define how identities are authenticated as discussed in [What is hybrid identity with Microsoft Entra ID?](#).

Selecting identity for an Azure Government application

When building any Azure application, you must first decide on the authentication technology:

- **Applications using modern authentication** – Applications using OAuth, OpenID Connect, and/or other modern authentication protocols supported by Microsoft Entra such as newly developed application built using PaaS technologies, for example, Web Apps, Azure SQL Database, and so on.
- **Applications using legacy authentication protocols (Kerberos/NTLM)** – Applications typically migrated from on-premises, for example, lift-and-shift applications.

Based on this decision, there are different considerations when building and deploying on Azure Government.

Applications using modern authentication in Azure Government

[Register an application with the Microsoft identity platform](#) shows how you can use Microsoft Entra ID to provide secure sign-in and authorization to your applications. This process is the same for Azure Public and Azure Government once you choose your identity authority.

Choosing your identity authority

Azure Government applications can use Microsoft Entra Government identities, but can you use Microsoft Entra Public identities to authenticate to an application hosted in Azure Government? Yes! Since you can use either identity authority, you need to choose which to use:

- **Microsoft Entra Public** – Commonly used if your organization already has a Microsoft Entra Public tenant to support Office 365 (Public or GCC) or another application.
- **Microsoft Entra Government** - Commonly used if your organization already has a Microsoft Entra Government tenant to support Office 365 (GCC High or DoD) or are creating a new tenant in Microsoft Entra Government.

Once decided, the special consideration is where you perform your app registration. If you choose Microsoft Entra Public identities for your Azure Government application, you must register the application in your Microsoft Entra Public tenant. Otherwise, if you perform the app registration in the directory the subscription trusts (Azure Government) the intended set of users can't authenticate.

Note

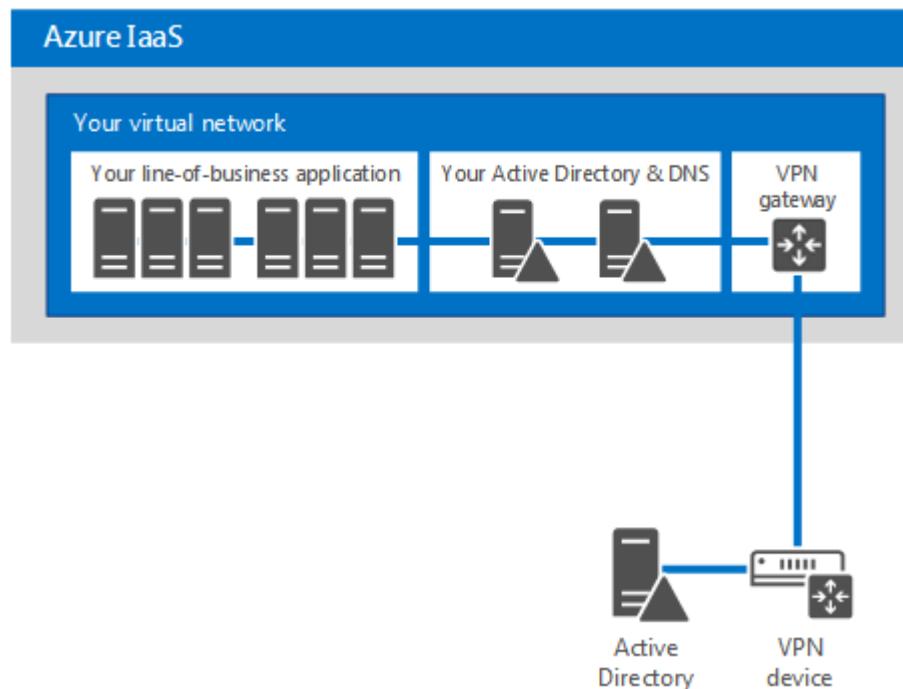
Applications registered with Microsoft Entra-only allow sign-in from users in the Microsoft Entra tenant the application was registered in. If you have multiple Microsoft Entra Public tenants, it's important to know which is intended to allow sign-ins from. If you intend to allow users to authenticate to the application from multiple Microsoft Entra tenants the application must be registered in each tenant.

The other consideration is the identity authority URL. You need the correct URL based on your chosen authority:

Identity authority	URL
Microsoft Entra Public	login.microsoftonline.com
Microsoft Entra Government	login.microsoftonline.us

Applications using legacy authentication protocols (Kerberos/NTLM)

Supporting Infrastructure-as-a-Service (IaaS) cloud-based applications dependent on NTLM/Kerberos authentication requires on-premises identity. The aim is to support logins for line-of-business application and other apps that require Windows integrated authentication. Adding Active Directory domain controllers as virtual machines in Azure IaaS is the typical method to support these types of apps, shown in the following figure:



ⓘ Note

The preceding figure is a simple connectivity example, using site-to-site VPN. Azure ExpressRoute is another and preferred connectivity option.

The type of domain controller to place in Azure is also a consideration based on application requirements for directory access. If applications require directory write access, deploy a standard domain controller with a writable copy of the Active Directory database. If applications only require directory read access, we recommend deploying a Read-Only Domain Controller (RODC) to Azure instead. Specifically, for RODCs we recommend following the guidance available at [Planning domain controller placement](#).

Documentation covering the guidelines for deploying Active Directory Domain Controllers and Active Director Federation Services (ADFS) is available from:

- [Safely virtualizing Active Directory Domain Services](#) answers questions such as
 - Is it safe to virtualize Windows Server Active Directory Domain Controllers?
 - Why deploy Active Directory to Azure Virtual Machines?
 - Can you deploy ADFS to Azure Virtual Machines?
- [Deploying Active Directory Federation Services in Azure](#) provides guidance on how to deploy ADFS in Azure.

Identity scenarios for subscription administration in Azure Government

First, see [Connect to Azure Government using portal](#) for instructions on accessing Azure Government management portal.

There are a few important points that set the foundation of this section:

- Azure subscriptions only trust one directory, therefore subscription administration must be performed by an identity from that directory.
- Azure Public subscriptions trust directories in Microsoft Entra Public whereas Azure Government subscriptions trust directories in Microsoft Entra Government.
- If you have both Azure Public and Azure Government subscriptions, separate identities for both are required.

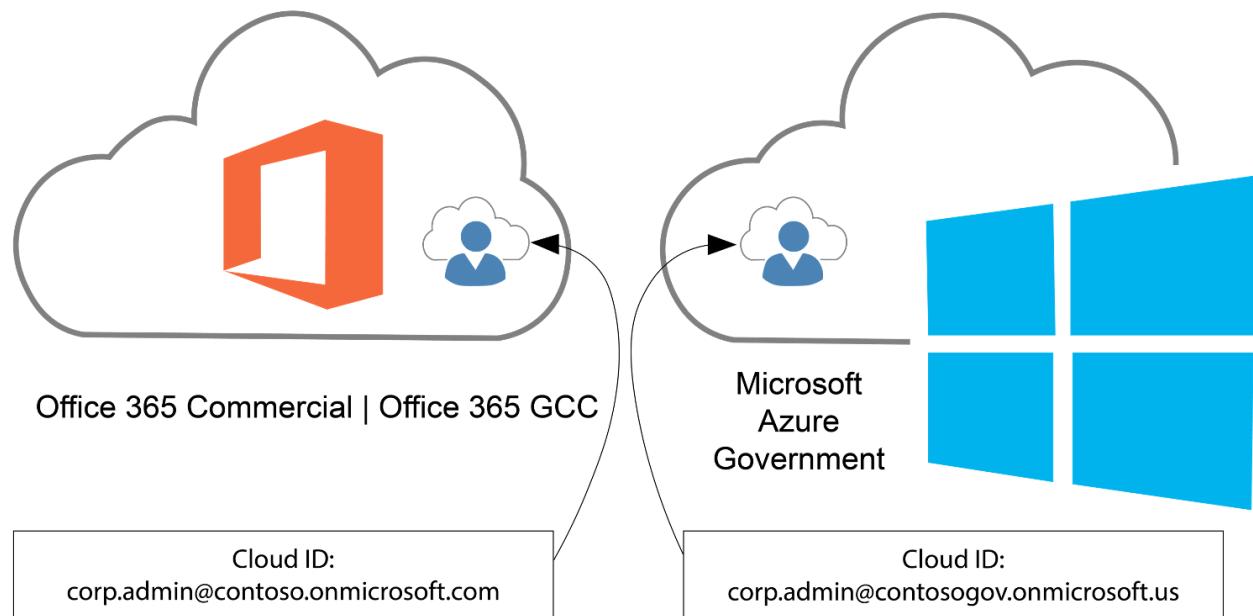
The currently supported identity scenarios to simultaneously manage Azure Public and Azure Government subscriptions are:

- Cloud identities - Cloud identities are used to manage both subscriptions.
- Hybrid and cloud identities - Hybrid identity for one subscription, cloud identity for the other.
- Hybrid identities - Hybrid identities are used to manage both subscriptions.

A common scenario, having both Office 365 and Azure subscriptions, is conveyed in the following sections.

Using cloud identities for multi-cloud subscription administration

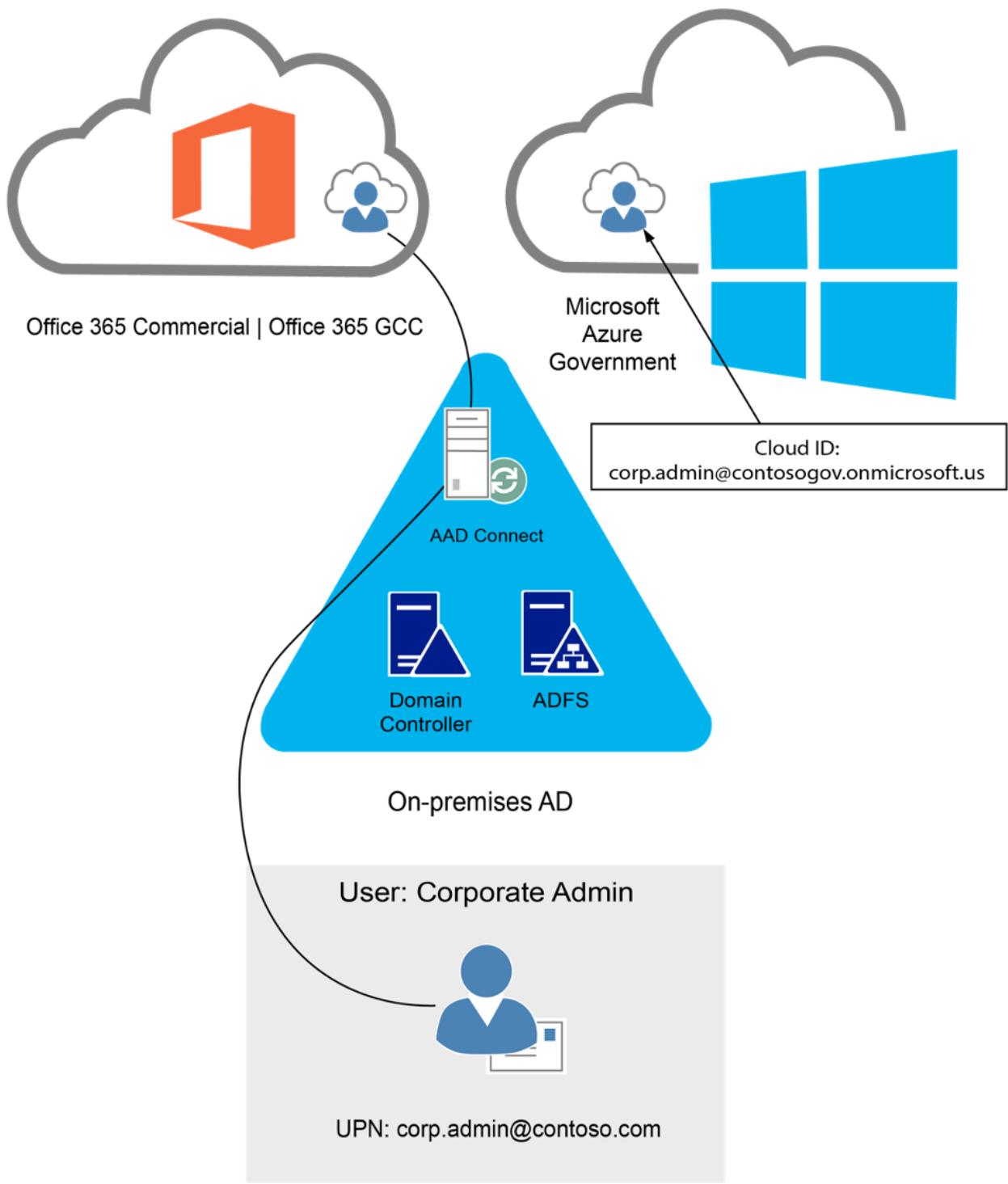
The following diagram is the simplest of the scenarios to implement.



While using cloud identities is the simplest approach, it is also the least secure because passwords are used as an authentication factor. We recommend [Microsoft Entra multifactor authentication](#), Microsoft's two-step verification solution, to add a critical second layer of security to secure access to Azure subscriptions when using cloud identities.

Using hybrid and cloud identities for multi-cloud subscription administration

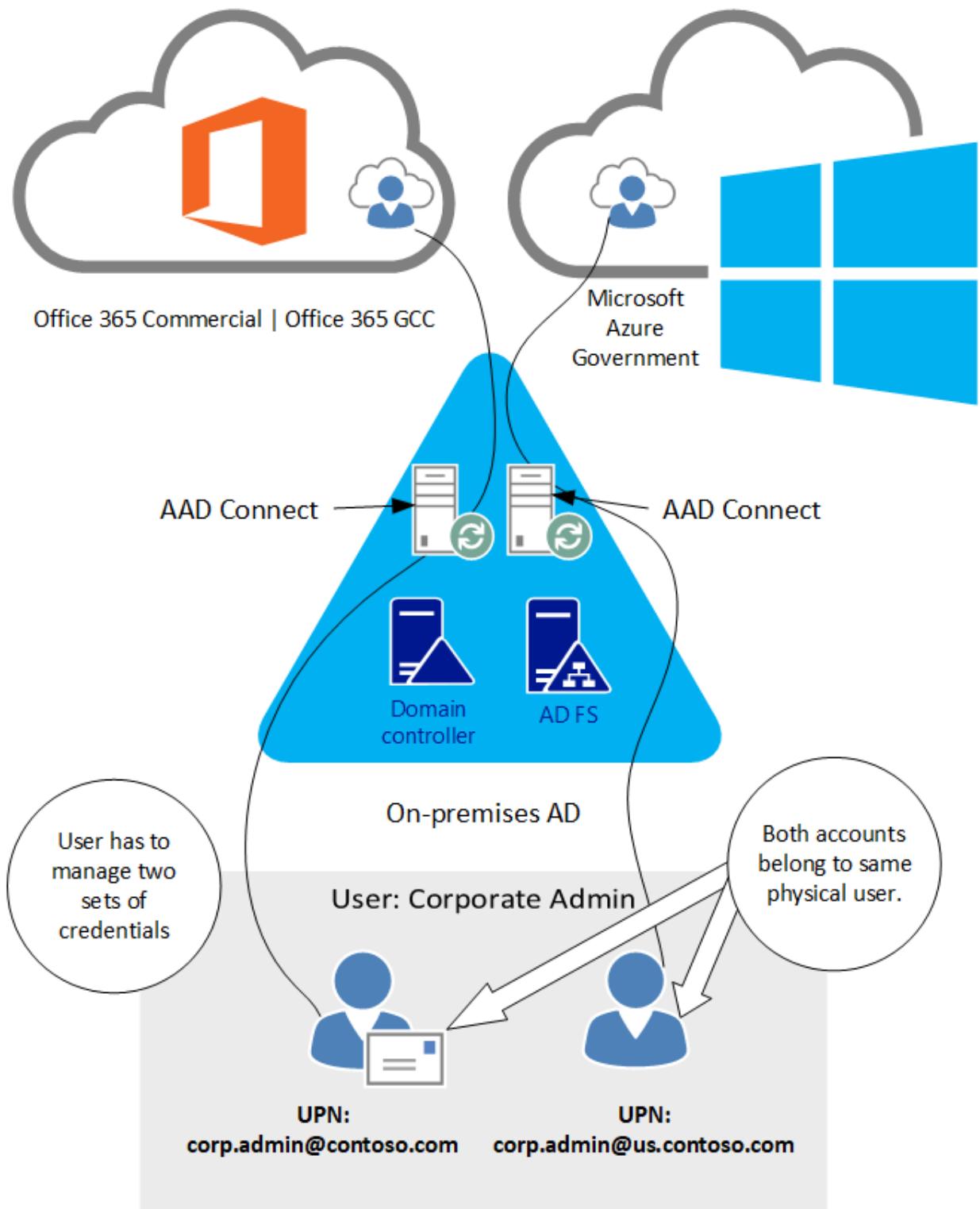
In this scenario, we include administrator identities through directory synchronization to the Public tenant while cloud identities are still used in the government tenant.



Using hybrid identities for administrative accounts allows the use of smartcards (physical or virtual). Government agencies using Common Access Cards (CACs) or Personal Identity Verification (PIV) cards benefit from this approach. In this scenario, ADFS serves as the identity provider and implements the two-step verification (for example, smart card + PIN).

Using hybrid identities for multi-cloud subscription administration

In this scenario, hybrid identities are used to administer subscriptions in both clouds.



Frequently asked questions

Why does Office 365 GCC use Microsoft Entra Public?

The first Office 365 US Government environment, Government Community Cloud (GCC), was created when Microsoft had a single cloud directory. The Office 365 GCC environment was designed to use Microsoft Entra Public while still adhering to controls and requirements outlined in FedRAMP Moderate, Criminal Justice Information Services (CJIS), Internal Revenue Service (IRS) 1075, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. Azure Government, with its

Microsoft Entra infrastructure, was created later. By that time, GCC had already secured the necessary compliance authorizations (for example, FedRAMP Moderate and CJIS) to meet Federal, State, and Local government requirements while serving hundreds of thousands of customers. Now, many Office 365 GCC customers have two Microsoft Entra tenants: one from the Microsoft Entra subscription that supports Office 365 GCC and the other from their Azure Government subscription, with identities in both.

How do I identify an Azure Government tenant?

Here's a way to find out using your browser of choice:

- Obtain your tenant name (for example, contoso.onmicrosoft.com) or a domain name registered to your Microsoft Entra tenant (for example, contoso.gov).
- Navigate to `https://login.microsoftonline.com/<domainname>/.well-known/openid-configuration`
 - `<domainname>` can either be the tenant name or domain name you gathered in the previous step.
 - **An example URL:**
`https://login.microsoftonline.com/contoso.onmicrosoft.com/.well-known/openid-configuration`
- The result posts back to the page in attribute/value pairs using JavaScript Object Notation (JSON) format that resembles:

JSON

```
{  
  "authorization_endpoint": "https://login.microsoftonline.com/b552ff1c-  
edad-4b6f-b301-5963a979bc4d/oauth2/authorize",  
  "tenant_region_scope": "USG"  
}
```

- If the `tenant_region_scope` attribute's value is **USG** as shown or **USGov**, you have yourself an Azure Government tenant.
 - The result is a JSON file that's natively rendered by more modern browsers such as Microsoft Edge, Mozilla Firefox, and Google Chrome. Internet Explorer doesn't natively render the JSON format so instead prompts you to open or save the file. If you must use Internet Explorer, choose the save option and open it with another browser or plain text reader.
 - The `tenant_region_scope` property is exactly how it sounds, regional. If you have a tenant in Azure Public in North America, the value would be **NA**.

If I'm an Office 365 GCC customer and want to build solutions in Azure Government do I need to have two tenants?

Yes, the Microsoft Entra Government tenant is required for your Azure Government subscription administration.

If I'm an Office 365 GCC customer that has built workloads in Azure Government, where should I authenticate from: Public or Government?

See [Choosing your identity authority](#) earlier in this article.

I'm an Office 365 customer and have chosen hybrid identity as my identity model. I also have several Azure subscriptions. Is it possible to use the same Microsoft Entra tenant to handle sign-in for Office 365, applications built in my Azure subscriptions, and/or applications reconfigured to use Microsoft Entra ID for sign-in?

Yes, see [Associate or add an Azure subscription to your Microsoft Entra tenant](#) to learn more about the relationship between Azure subscriptions and Microsoft Entra ID. It also contains instructions on how to associate subscriptions to the common directory of your choosing.

Can an Azure Government subscription be associated with a directory in Microsoft Entra Public?

No, the ability to manage Azure Government subscriptions requires identities sourced from a directory in Microsoft Entra Government.

Next steps

- [Azure Government developer guide](#)
- [Azure Government security](#)
- [Azure Government compliance](#)
- [Compare Azure Government and global Azure](#)
- [Multi-tenant user management](#)
- [Microsoft Entra fundamentals documentation](#)

Integrate Microsoft Entra authentication with Web Apps on Azure Government

Article • 10/12/2023

The following quickstart helps you get started integrating Microsoft Entra authentication with applications on Azure Government. Microsoft Entra authentication on Azure Government is similar to the Azure commercial platform, with a [few exceptions](#).

Learn more about [Microsoft Entra authentication Scenarios](#).

Integrate Microsoft Entra login into a web application using OpenID Connect

This section shows how to integrate Microsoft Entra ID using the OpenID Connect protocol for signing in users into a web app.

Prerequisites

- A Microsoft Entra tenant in Azure Government. You must have an [Azure Government subscription](#) in order to have a Microsoft Entra tenant in Azure Government. For more information on how to get a Microsoft Entra tenant, see [How to get a Microsoft Entra tenant](#)
- A user account in your Microsoft Entra tenant. This sample does not work with a Microsoft account, so if you signed in to the Azure Government portal with a Microsoft account and have never created a user account in your directory before, you need to do that now.
- Have an [ASP.NET Core application deployed and running in Azure Government](#)

Step 1: Register your web application with your Microsoft Entra tenant

1. Sign in to the [Azure Government portal](#).
2. On the top bar, click on your account and under the Directory list, choose the Active Directory tenant where you wish to register your application.
3. Click on All Services in the left-hand nav, and choose Microsoft Entra ID.
4. Click on App registrations and choose Add.

5. Enter the name for your application, and select 'Web Application and/or Web API' as the Application Type. For the sign-on URL, enter the base URL for your application, which is your Azure App URL + "/signin-oidc."

 **Note**

If you have not deployed your application and want to run it locally, your App URL would be your local host address.

Click on **Create** to create the application.

6. While still in the Azure portal, choose your application, click on **Settings**, and choose **Properties**.
7. Find the Application ID value and copy it to the clipboard.
8. For the App ID URI, enter `https://<your_tenant_name>/<name_of_your_app>`, replacing `<your_tenant_name>` with the name of your Microsoft Entra tenant and `<name_of_your_app>` with the name of your application.

Step 2: Configure your app to use your Microsoft Entra tenant

Azure Government Variations

The only variation when setting up Microsoft Entra Authorization on the Azure Government cloud is in the Microsoft Entra Instance:

- "https://login.microsoftonline.us"

Configure the InventoryApp project

1. Open your application in Visual Studio 2019.
2. Open the `appsettings.json` file.
3. Add an `Authentication` section and fill out the properties with your Microsoft Entra tenant information.

C#

```
//ClientId: Azure AD-> App registrations -> Application ID
//Domain: <tenantname>.onmicrosoft.us
```

```
//TenantId: Azure AD -> Properties -> Directory ID

"Authentication": {
  "AzureAd": {

    "Azure ADInstance": "https://login.microsoftonline.us/",
    "CallbackPath": "/signin-oidc",
    "ClientId": "<clientid>",
    "Domain": "<domainname>",
    "TenantId": "<tenantid>"
  }
}
```

4. Fill out the `ClientId` property with the Client ID for your app from the Azure Government portal. You can find the Client ID by navigating to Microsoft Entra ID -> App Registrations -> Your Application -> Application ID.
5. Fill out the `TenantId` property with the Tenant ID for your app from the Azure Government portal. You can find the Tenant ID by navigating to Microsoft Entra ID -> Properties -> Directory ID.
6. Fill out the `Domain` property with `<tenantname>.onmicrosoft.us`.
7. Open the `startup.cs` file.
8. In your `ConfigureServices` method, add the following code:

```
C#
```

```
public void ConfigureServices(IServiceCollection services)
{
  //Add Azure AD authentication
  services.AddAuthentication(options => {
    options.DefaultScheme =
CookieAuthenticationDefaults.AuthenticationScheme;
    options.DefaultChallengeScheme =
OpenIdConnectDefaults.AuthenticationScheme;
  })
  .AddCookie()
  .AddOpenIdConnect(options => {
    options.Authority =
Configuration["Authentication:AzureAd:Azure ADInstance"] +
Configuration["Authentication:AzureAd:TenantId"];
    options.ClientId =
Configuration["Authentication:AzureAd:ClientId"];
    options.CallbackPath =
Configuration["Authentication:AzureAd:CallbackPath"];
  });
}
```

In the same file, add this one line of code to the `Configure` method:

C#

```
app.UseAuthentication();
```

9. Navigate to your **Home** controller or whichever controller file is your home page, **where you want your users to log in**. Add the `[Authorize]` tag before the class definition.

Next steps

- Navigate to the [Azure Government PaaS Sample](#) to see Microsoft Entra authentication as well as other services being integrated in an Application running on Azure Government.
- Subscribe to the [Azure Government blog](#)
- Get help on Stack Overflow by using the "[azure-gov](#)" tag

Deploy an app in Azure Government with Azure Pipelines

Article • 05/11/2023

This how-to guide helps you use Azure Pipelines to set up continuous integration (CI) and continuous delivery (CD) of your web app running in Azure Government. CI/CD automates the build of your code from a repository along with the deployment (release) of the built code artifacts to a service or set of services in Azure Government. In this how-to guide, you'll build a web app and deploy it to an Azure Government App Service. The build and release process is triggered by a change to a code file in the repository.

ⓘ Note

Azure DevOps isn't available on Azure Government. While this how-to guide shows how to configure the CI/CD capabilities of Azure Pipelines to deploy an app to a service inside Azure Government, be aware that Azure Pipelines runs its pipelines outside of Azure Government. Research your organization's security and service policies before using it as part of your deployment tools. For guidance on how to use Azure DevOps Server to create a DevOps experience inside a private network on Azure Government, see [Azure DevOps Server on Azure Government](#).

Azure Pipelines is used by development teams to configure continuous deployment for applications hosted in Azure subscriptions. We can use this service for applications running in Azure Government by defining [service connections](#) for Azure Government.

ⓘ Note

We recommend that you use the Azure Az PowerShell module to interact with Azure. See [Install Azure PowerShell](#) to get started. To learn how to migrate to the Az PowerShell module, see [Migrate Azure PowerShell from AzureRM to Az.](#)

Prerequisites

Before starting this how-to guide, you must complete the following prerequisites:

- [Create an organization in Azure DevOps](#)
- [Create and add a project to the Azure DevOps organization](#)

- Install and set up [Azure PowerShell](#)

If you don't have an active Azure Government subscription, create a [free account](#) before you begin.

Create Azure Government App Service app

Follow [Tutorial: Deploy an Azure App Service app](#) to learn how to deploy an Azure App Service app to Azure Government. The following steps will set up a CI/CD process to deploy to your web app.

Set up build and source control integration

Review one of the following quickstarts to set up a build for your specific type of app:

- [ASP.NET 4](#)
- [.NET Core](#)
- [Node.js](#)

Generate a service principal

1. Copy and paste the following service principal creation PowerShell script into an IDE or editor, and then save the script. This code is compatible only with Azure Az PowerShell v7.0.0 or higher.

```
PowerShell

param
(
    [Parameter(Mandatory=$true, HelpMessage="Enter Azure subscription
name - you need to be subscription admin to execute the script")]
    [string] $subscriptionName,
    [Parameter(Mandatory=$false, HelpMessage="Provide SPN role
assignment")]
    [string] $spnRole = "owner",
    [Parameter(Mandatory=$false, HelpMessage="Provide Azure environment
name for your subscription")]
    [string] $environmentName = "AzureUSGovernment"
)
# Initialize
$ErrorActionPreference = "Stop"
$VerbosePreference = "SilentlyContinue"
$userName = ($env:USERNAME).Replace(' ', '')
```

```

$newguid = [guid]::NewGuid()
$displayName = [String]::Format("AzDevOps.{0}.{1}", $userName,
$newguid)
$homePage = "http://" + $displayName
$identifierUri = $homePage

# Check for Azure Az PowerShell module
$isAzureModulePresent = Get-Module -Name Az -ListAvailable
if ([String]::IsNullOrEmpty($isAzureModulePresent) -eq $true)
{
    Write-Output "Script requires Azure PowerShell modules to be
present. Obtain Azure PowerShell from
https://learn.microsoft.com/powershell/azure/install-az-ps" -Verbose
    return
}

Import-Module -Name Az.Accounts
Write-Output "Provide your credentials to access your Azure
subscription $subscriptionName" -Verbose
Connect-AzAccount -Subscription $subscriptionName -Environment
$environmentName
$azureSubscription = Get-AzSubscription -SubscriptionName
$subscriptionName
$connectionName = $azureSubscription.Name
$tenantId = $azureSubscription.TenantId
$id = $azureSubscription.SubscriptionId

# Create new Azure AD application
Write-Output "Creating new application in Azure AD (App URI -
$identifierUri)" -Verbose
$azureAdApplication = New-AzADApplication -DisplayName $displayName -
HomePage $homePage -Verbose
$appId = $azureAdApplication.AppId
$objectId = $azureAdApplication.Id
Write-Output "Azure AD application creation completed successfully
(Application Id: $appId) and (Object Id: $objectId)" -Verbose

# Add secret to Azure AD application
Write-Output "Creating new secret for Azure AD application"
$secret = New-AzADAppCredential -ObjectId $objectId -EndDate (Get-
Date).AddYears(2)
Write-Output "Secret created successfully" -Verbose

# Create new SPN
Write-Output "Creating new SPN" -Verbose
$spn = New-AzADServicePrincipal -ApplicationId $appId
$spnName = $spn.DisplayName
Write-Output "SPN creation completed successfully (SPN Name: $spnName)"
-Verbose

# Assign role to SPN
Write-Output "Waiting for SPN creation to reflect in directory before
role assignment"
Start-Sleep 20
Write-Output "Assigning role ($spnRole) to SPN app ($appId)" -Verbose

```

```

New-AzRoleAssignment -RoleDefinitionName $spnRole -ApplicationId
$spn.AppId
Write-Output "SPN role assignment completed successfully" -Verbose

# Print values
Write-Output "`nCopy and paste below values for service connection" -
Verbose
Write-Output
"*****"
Write-Output "Connection Name: $connectionName(SPN)"
Write-Output "Environment: $environmentName"
Write-Output "Subscription Id: $id"
Write-Output "Subscription Name: $connectionName"
Write-Output "Service Principal Id: $appId"
Write-Output "Tenant Id: $tenantId"
Write-Output
"*****"
*****

```

2. Open your PowerShell window and run the following command, which sets a policy that enables running local files:

```
Set-ExecutionPolicy -Scope Process -ExecutionPolicy Bypass
```

When asked whether you want to change the execution policy, enter "A" (for "Yes to All").

3. Navigate to the directory where you saved the service principal creation PowerShell script.
 4. Edit the following command with the name of your script and run:
- ```
./<name of script file you saved>
```
5. The "subscriptionName" parameter can be found by logging into your Azure Government subscription via `Connect-AzAccount -EnvironmentName AzureUSGovernment` and then running `Get-AzureSubscription`.
  6. After providing your Azure Government subscription credentials, you should see the following message:
- ```
The Environment variable should be AzureUSGovernment
```
7. After the script has run, you should see your service connection values. Copy these values as we'll need them when setting up our endpoint.

```
SPN role assignment completed successfully
Copy and paste below values for service connection
*****
Connection Name: Demo(SPN)
Environment: AzureUSGovernment
Subscription Id: [REDACTED]
Subscription Name: Demo
Service Principal Id: [REDACTED]
Tenant Id: [REDACTED]
*****
*****
```

Configure the Azure Pipelines service connection

Follow [Manage service connections](#) to set up the Azure Pipelines service connection.

Make one change specific to Azure Government:

- In step #3 of [Manage service connections: Create a service connection](#), click on *Use the full version of the service connection catalog* and set **Environment** to **AzureUSGovernment**.

Define a release process

Follow [Deploy an Azure Web App](#) instructions to set up your release pipeline and deploy to your application in Azure Government.

Q&A

Do I need a build agent?

You need at least one [agent](#) to run your deployments. By default, the build and deployment processes are configured to use [hosted agents](#). Configuring a private agent would limit data sharing outside of Azure Government.

Can I configure CD on Azure DevOps Server (formerly Team Foundation Server) to target Azure Government?

You can set up Azure DevOps Server in Azure Government. For guidance on how to use Azure DevOps Server to create a DevOps experience inside a private network on Azure Government, see [Azure DevOps Server on Azure Government](#).

Next steps

For more information, see the following resources:

- Sign up for Azure Government trial ↗
- Acquiring and accessing Azure Government ↗
- Ask questions via the `azure-gov` tag on StackOverflow ↗
- Azure Government blog ↗
- What is Infrastructure as Code? – Azure DevOps
- DevSecOps for infrastructure as code (IaC) – Azure Architecture Center
- Azure Government overview
- Azure Government security
- Compare Azure Government and global Azure
- Azure Government compliance
- Azure compliance

App Service Environment reference for DoD customers connected to the DISA CAP

Article • 04/09/2023

This article explains the baseline configuration of an App Service Environment (ASE) with an internal load balancer (ILB) for customers who use the Defense Information Systems Agency (DISA) Cloud Access Point (CAP) to connect to Azure Government.

Environment configuration

Assumptions

You've deployed an ASE with an ILB and have implemented an ExpressRoute connection to the DISA CAP.

Route table

When you create the ASE via the Azure Government portal, a route table with a default route of 0.0.0.0/0 and next hop "Internet" is created. However, since DISA advertises a default route out of the ExpressRoute circuit, the User Defined Route (UDR) should either be deleted, or you should remove the default route to Internet.

You'll need to create new routes in the UDR for the management addresses to keep the ASE healthy. For Azure Government ranges, see [App Service Environment management addresses](#).

- 23.97.29.209/32 -> Internet
- 13.72.53.37/32 -> Internet
- 13.72.180.105/32 -> Internet
- 52.181.183.11/32 -> Internet
- 52.227.80.100/32 -> Internet
- 52.182.93.40/32 -> Internet
- 52.244.79.34/32 -> Internet
- 52.238.74.16/32 -> Internet

Make sure the UDR is applied to the subnet your ASE is deployed to.

Network security group (NSG)

The ASE will be created with the following inbound and outbound security rules. The inbound security rules **must** allow ports 454-455 with an ephemeral source port range (*). The following images describe the default NSG rules generated during the ASE creation. For more information, see [Networking considerations for an App Service Environment](#).

Inbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	...
100	Inbound-management	454-455	Any	Any	Any	Allow	...
110	ASE-internal-inbound	Any	Any	192.168.250.0/24	Any	Allow	...
120	Inbound-HTTP	80	Any	Any	Any	Allow	...
130	Inbound-HTTPS	443	Any	Any	Any	Allow	...
140	Inbound-FTP	21	Any	Any	Any	Allow	...
150	Inbound-FTPS	990	Any	Any	Any	Allow	...
160	Inbound-FTP-Data	10001-10020	Any	Any	Any	Allow	...
170	Inbound-Remote-Debugging	4016-4022	Any	Any	Any	Allow	...
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow	...
65500	DenyAllInBound	Any	Any	Any	Any	Deny	...

Outbound security rules

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION	...
100	Outbound-443	443	Any	Any	Any	Allow	...
110	Outbound-SMB	445	Any	Any	Any	Allow	...
120	Outbound-DB	1433	Any	Any	Any	Allow	...
130	Outbound-DB2	11000-11999	Any	Any	Any	Allow	...
140	Outbound-DB3	14000-14999	Any	Any	Any	Allow	...
150	Outbound-DNS	53	Any	Any	Any	Allow	...
160	ASE-internal-outbound	Any	Any	Any	192.168.250.0/24	Allow	...
170	Outbound-80	80	Any	Any	Any	Allow	...
180	ASE-to-VNET	Any	Any	Any	192.168.250.0/23	Allow	...
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow	...
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow	...
65500	DenyAllOutBound	Any	Any	Any	Any	Deny	...

Service endpoints

Depending on the storage you use, you need to enable service endpoints for Azure SQL Database and Azure Storage to access them without going back to the DISA CAP. You also need to enable the Event Hubs service endpoint for ASE logs. For more information, see [Networking considerations for App Service Environment: Service endpoints](#).

FAQs

How long will it take for configuration changes to take effect?

Some configuration changes may take time to become effective. Allow several hours for changes to routing, NSGs, ASE Health, and so on, to propagate and take effect. Otherwise, you can optionally reboot the ASE.

Azure Resource Manager template sample

ⓘ Note

To deploy non-RFC 1918 IP addresses in the portal, you must pre-stage the VNet and subnet for the ASE. You can use an Azure Resource Manager template to deploy the ASE with non-RFC1918 IPs as well.



This template deploys an **ILB ASE** into the Azure Government or DoD regions.

Next steps

- [Sign up for Azure Government trial](#) ↗
- [Acquiring and accessing Azure Government](#) ↗
- [Ask questions via the azure-gov tag on StackOverflow](#) ↗
- [Azure Government blog](#) ↗
- [Azure Government overview](#)
- [Azure Government security](#)
- [Azure Government compliance](#)
- [Secure Azure computing architecture](#)
- [Azure Policy overview](#)
- [Azure Policy regulatory compliance built-in initiatives](#)
- [Azure Government services by audit scope](#)
- [Azure Government isolation guidelines for Impact Level 5 workloads](#)
- [Azure Government DoD overview](#)

Azure Government cybersecurity: Monitoring and securing your assets with Azure Monitor logs

Article • 12/31/2021

Cybersecurity in the cloud

A crucial concern for our customers who are moving to the cloud is retaining asset management and security of the Azure Government services that they've deployed to the cloud. Virtual machine firewalls need to be configured correctly. Virtual networks need to have the right network security groups applied to them. Access to your assets needs to be locked down at the right time. All these necessary work streams need to be planned, designed, and provisioned to enable a secure infrastructure for your agency to use.

Setting up this kind of environment can be challenging. Onboarding your fleet of servers to any monitoring service is a hard operation to scale, and it can also be challenging to update the monitoring service. Monitoring infrastructure on different cloud providers, and across the cloud and on-premises is difficult. Finally, keeping your monitoring up-to-date and enabling Azure Application Insights to monitor, detect, alert, and counter cybersecurity threats require time, resources, and computing power.

Azure Monitor logs

Azure Monitor logs, now available in Azure Government, uses hyperscale log search to quickly analyze your data and expose threats in your environment. This article focuses on using Azure Monitor logs that uses hyperscale log search to quickly analyze your data and expose threats in your environment.

Note

This article was recently updated to use the term Azure Monitor logs instead of Log Analytics. Log data is still stored in a Log Analytics workspace and is still collected and analyzed by the same Log Analytics service. We are updating the terminology to better reflect the role of **logs** in Azure Monitor. See [Azure Monitor terminology changes](#) for details.

Azure Monitor logs can:

- Deploy agents to individual VMs (Linux and Windows) on Azure, other cloud providers, and on-premises.
- Connect your existing logs via an Azure Government storage account or System Center Operations Manager endpoint with existing logging data.

Let's explore how we can get Azure Monitor logs integrated into your fleet and look at some of the out-of-box solutions that address the concerns that we've described here.

Onboarding servers to Azure Monitor logs

The first step in integrating your cloud assets with Azure Monitor logs is installing the Log Analytics agent across log sources. For virtual machines, this is simple because you can manually download the agent from the Azure Monitor logs portal.

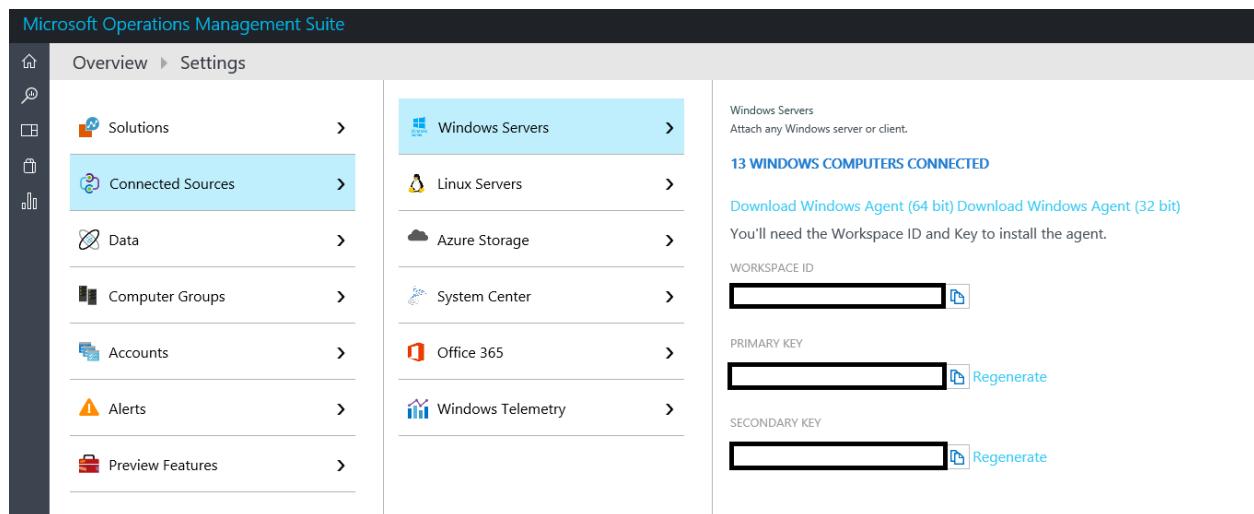


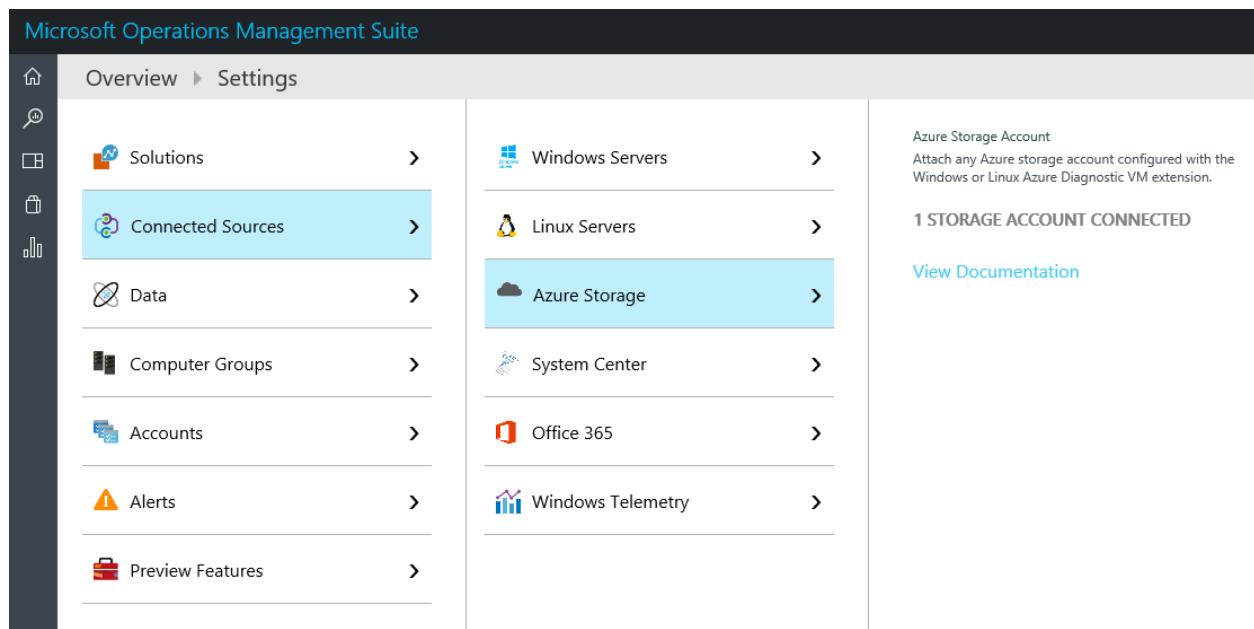
Figure 1: Windows servers connected to Azure Monitor logs

You can connect Azure VMs to Azure Monitor logs directly through the Azure portal. For instructions, see [New ways to enable Azure Monitor logs on your Azure VMs](#).

You can also connect them programmatically or configure the Azure Monitor virtual machine extension right into your Azure Resource Manager templates. See the instructions for Windows-based machines at [Connect Windows computers to Azure Monitor logs](#) and for Linux-based machines at [Connect Linux computers to Azure Monitor logs](#).

Onboarding storage accounts and Operations Manager to Azure Monitor logs

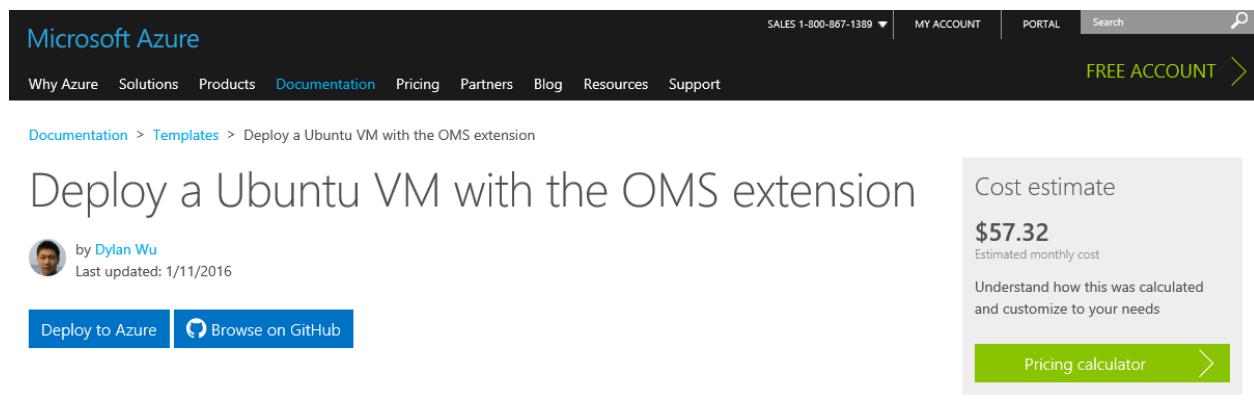
Azure Monitor logs can also connect to your storage account and/or existing System Center Operations Manager deployments to offer you operations management in hybrid scenarios (across cloud providers or in cloud/on-premises infrastructures).



The screenshot shows the Microsoft Operations Management Suite interface. The left sidebar has icons for Home, Search, Connected Sources, Data, Computer Groups, Accounts, Alerts, and Preview Features. The main area has sections for Windows Servers, Linux Servers, Azure Storage, System Center, Office 365, and Windows Telemetry. The 'Connected Sources' section is highlighted. On the right, there is a 'Azure Storage Account' section with a link to 'View Documentation'.

Figure 2: Connecting Azure Storage and Operations Manager to Azure Monitor logs

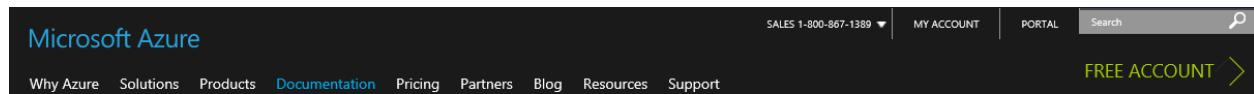
Azure Monitor logs also supports collecting logging information from other monitoring services like Chef or Puppet. Furthermore, for Azure deployments, we have VMs with Azure Monitor logs-enabled Azure Resource Manager templates so you can deploy compute and onboard to your Log Analytics workspace at the same time.



The screenshot shows the Microsoft Azure Documentation page for 'Deploy a Ubuntu VM with the OMS extension'. It includes a navigation bar with links to Why Azure, Solutions, Products, Documentation, Pricing, Partners, Blog, Resources, and Support. A search bar and a 'FREE ACCOUNT' button are also present. The main content area shows the title 'Deploy a Ubuntu VM with the OMS extension' and a bio for Dylan Wu. It includes buttons for 'Deploy to Azure' and 'Browse on GitHub'. To the right, there is a 'Cost estimate' section showing '\$57.32' and a 'Pricing calculator' button.

This template allows you to deploy a Ubuntu VM with the OMS extension installed and onboarded to a specified workspace

This Azure Resource Manager (ARM) template was created by a member of the community and not by Microsoft. Each ARM template is licensed to you under a license agreement by its owner, not Microsoft. Microsoft is not responsible for ARM templates provided and licensed by community members and does not screen for security, compatibility, or performance. Community ARM templates are not supported under any Microsoft support program or service, and are made available AS IS without warranty of any kind.



The screenshot shows the Microsoft Azure Documentation page. At the top, there are links for 'SALES 1-800-867-1389', 'MY ACCOUNT', 'PORTAL', and a 'Search' bar. On the right, there is a 'FREE ACCOUNT' button. The main content area has a title 'Deploy a Windows VM with the OMS extension' and a sub-section 'Cost estimate' showing '\$0.07'. Below the title, there are buttons for 'Deploy to Azure' and 'Browse on GitHub'. The page also includes a brief description of the template and a note about the license.

Documentation > Templates > Deploy a Windows VM with the OMS extension

Deploy a Windows VM with the OMS extension



by Dylan Wu
Last updated: 1/11/2016

[Deploy to Azure](#)

[Browse on GitHub](#)

Cost estimate

\$0.07

Estimated monthly cost

Understand how this was calculated
and customize to your needs

[Pricing calculator](#)

This template allows you to deploy a Windows VM with the OMS extension installed and onboarded to a specified workspace

This Azure Resource Manager (ARM) template was created by a member of the community and not by Microsoft. Each ARM template is licensed to you under a license agreement by its owner, not Microsoft. Microsoft is not responsible for ARM templates provided and licensed by community members and does not screen for security, compatibility, or performance. Community ARM templates are not supported under any Microsoft support program or service, and are made available AS IS without warranty of any kind.

Figure 3: Azure Resource Manager templates for Azure VMs with Azure Monitor VM extension

Information about setting up Azure Monitor logs with your existing Operations Manager implementation on-premises can be found in [Connect Operations Manager to Azure Monitor logs](#).

Applying intelligence through management solutions

Now that you have various sources for logging data, you have to make sense of all this data.

Azure Monitor logs, at its core, is a log search service that lets you write powerful queries to quickly search across thousands or even millions of logs. However, discovering the issues that you need to write queries can be difficult.

Enter Azure Monitor logs solutions. These are packs of queries that are natively integrated with Azure Monitor logs to proactively give you insights into your Azure Monitor logs-managed fleet.

On the theme of cyber security, I briefly discuss three cybersecurity scenarios that Azure Monitor logs can solve out of the box for you.

Antimalware assessment

Antimalware assessments give you a canned set of queries, notifications, and monitoring dashboards to tell you at a glance how well your fleet is protected against malware.

This dashboard gives you a list of four things:

- Any servers that have active and/or remediated threats.
- Currently detected threats.
- Computers that aren't being sufficiently protected. Azure Monitor logs finds this information by crawling the logs of your computers to look for any site of FWs that are being opened, or for improperly configured rules in common web browsers.
- Analysis of how your protected servers are being protected, for example by native Windows OS virus protection or a solution such as System Center Endpoint Protection.

For example, you can see that the following threat was caught and automatically triaged by System Center:

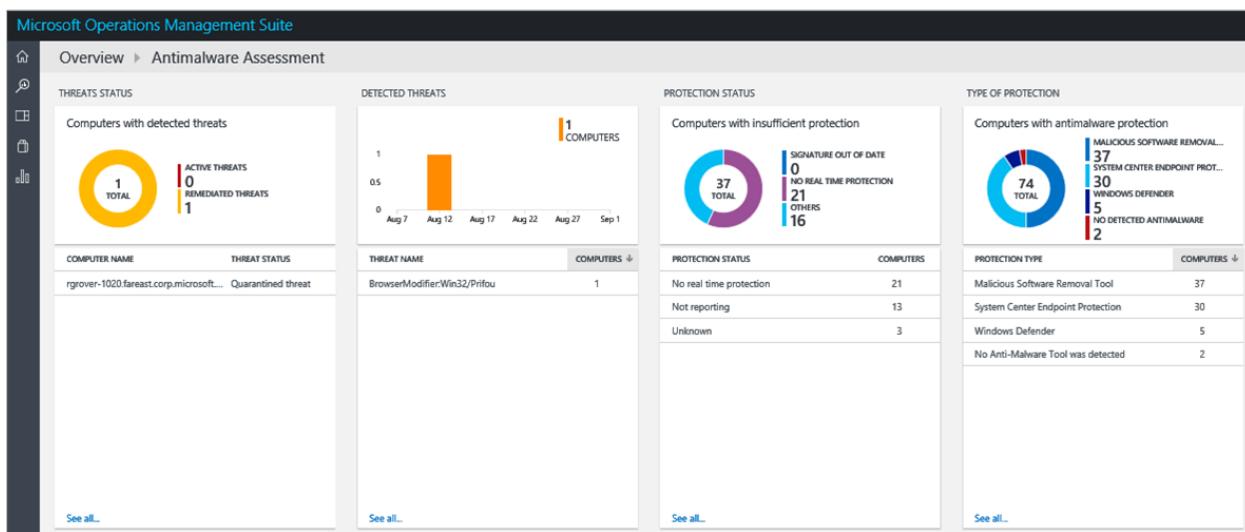


Figure 4: Azure Monitor logs antimalware assessment solution

More information about antimalware assessment can be found in the article [Malware assessment solution in Azure Monitor logs](#).

Identity and access

Another common cybersecurity scenario in the cloud revolves around credential compromise. Not only does your cloud subscription have credentials, but each individual VM has a user and/or secret (usually a certificate or password) that's associated with it.

Azure Monitor logs organizes all sign-in attempts in your fleet and buckets them depending on type (remote, local, username, and so on). For example, in the following example, I can see a large amount of unsuccessful sign-in attempts from largely random strings as usernames. This indicates that it's highly likely that my computers have been exposed and not properly protected by firewalls and access control lists.

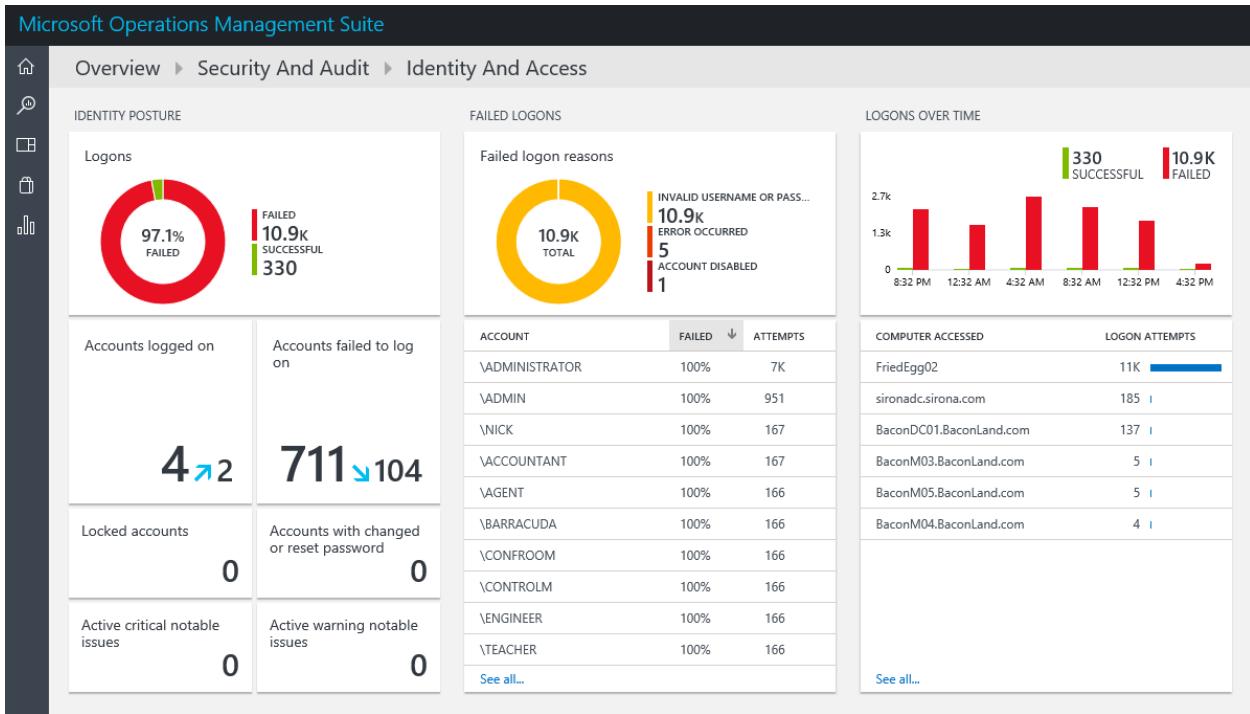


Figure 5: 97.3% sign-ins failed in the last 24 hours

Threat intelligence

Azure Monitor logs also provides protection against malicious insider scenarios, when there's a security compromise inside your organization and a malicious user is trying to exfiltrate data.

Azure Monitor logs threat intelligence looks at all the network logs on your computer and automatically searches for and notifies you about inbound/outbound network connections to known malicious IPs (for example, IP addresses on the unindexed dark net).

For example, in the following screenshot, I can see that there are both inbound and outbound network connections to the People's Republic of China.

By double-clicking the inbound tag, I discover that a Linux VM that is being managed by Azure Monitor logs is making outbound connections to a known dark net IP address in China.

You can also set up alerts to Azure Monitor logs solutions like threat intelligence. In the following screenshot, I've set up an alert so that if Azure Monitor logs detects more than 10 outbound connections to a known malicious IP address, it sends an alert out to me via email. I then configure that alert to fire an Azure Automation job, which is set up to automatically shut down that VM.

Microsoft Operations Management Suite

Log Search > Add Alert Rule

General

Alert information

Name: OutboundConnectionRule

Description:

Severity: Critical

Search query: Use current search query

```
MaliciousIP="61.240.144.65" AND (RemoteIPCountry=" OR MaliciousIPCountry=") AND ((Type=WireData AND Direction=Outbound) OR (Type=CommonSecurityLog AND CommunicationDirection=Outbound))
```

Time window: 15 Minutes

This search returned 0 results for the time window selected

Schedule

Alert frequency: Check for this alert every 15 Minutes

Generate alert based on: Number of results Greater than 10

Suppress alerts: When checked, allows you to set an amount of time to wait before alerting again to reduce alert noise

Actions

Email notification

Subject: ALERT - Critical - OutboundConnectionRule

Recipients (semi-colon separated): sacha@microsoft.com

Webhook

Runbook

Automation account: goforum2016-automation

Select a runbook: vm-auto-shutdown

Run on: Azure

Figure 6: Azure Monitor logs alerts and automation

This is just one example of an out-of-the-box Azure Monitor logs solution that can be applied to your fleet, whether it's running on Azure, another cloud service provider, or on-premises.

Azure Monitor continues to update its machine learning to fight the latest threats automatically for you, and we continue to roll out new solutions to the Azure marketplace as well.

For more information about Azure Monitor logs, see [our documentation page](#).

Azure Government Marketplace

Article • 11/10/2021

Azure Government Marketplace helps connect government agencies and partners with independent software vendors (ISVs) and start-ups that are offering their solutions in Azure Government.

ⓘ Note

For information on making your images available in Azure Government, see the [partner onboarding guidelines](#).

Variations

Azure Government Marketplace differs from Azure Marketplace in the following ways:

- Only Bring Your Own License (BYOL) and Pay-as-you-Go (PayGo) images are available.
- A different set of images is available. For a list of available images, see [Azure Government Marketplace images](#).

ⓘ Note

Red Hat Enterprise Linux is available in Azure Government with Azure Marketplace billing. This offering is a special case exception to the above statement about license options in Azure Government.

Enable the Azure Government Marketplace

If your subscription is under an Enterprise Agreement (EA), the Azure Government Marketplace must be enabled before you can deploy a Marketplace solution to your subscription.

1. Log in to the [Enterprise Account Portal](#) as an Enterprise Administrator
2. Navigate to **Manage**
3. Under **Enrollment Details**, click the pencil icon next to the **Azure Marketplace** line item
4. Toggle **Enabled/Disabled** as appropriate

5. Click Save

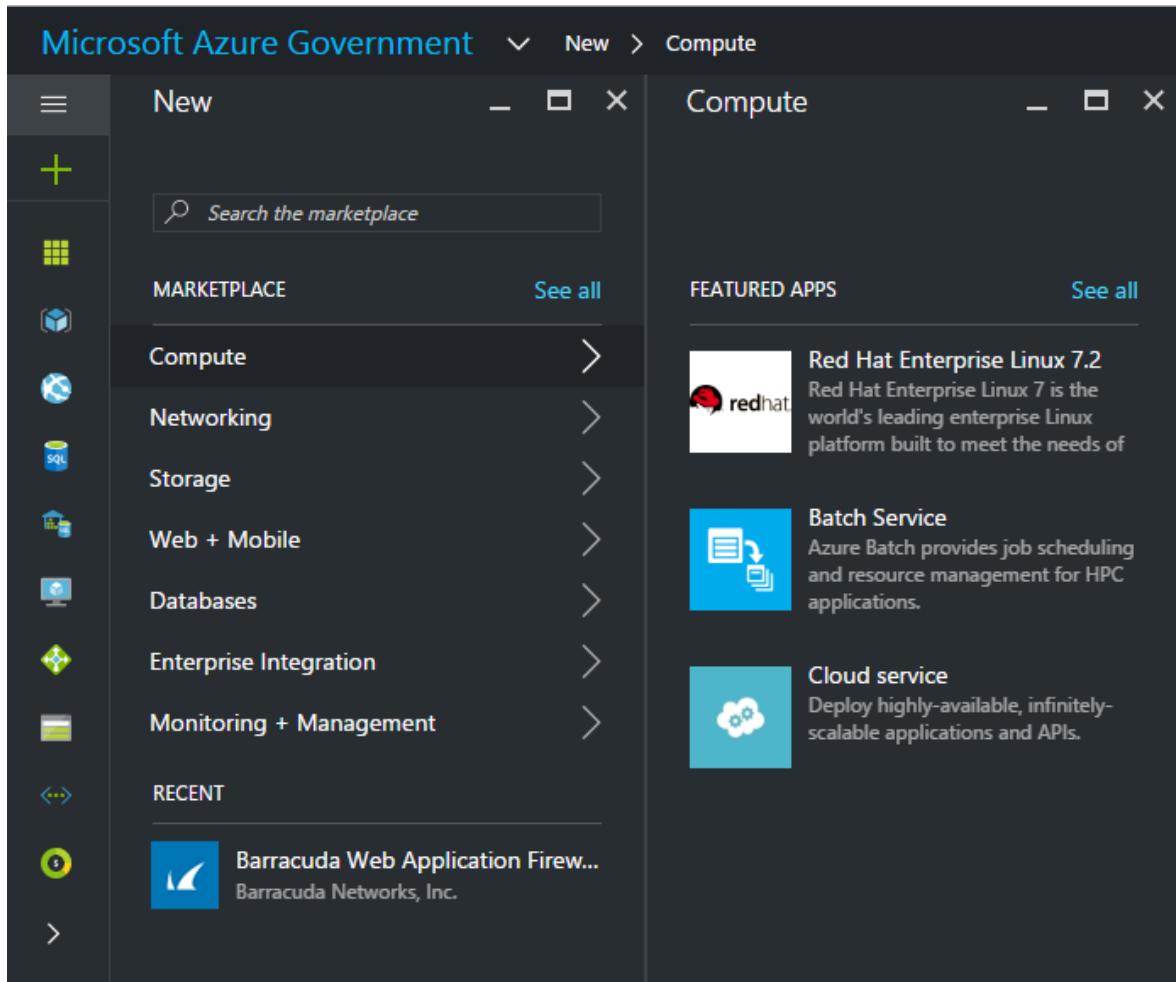
① Note

It can take up to 24 hours for the change to take effect.

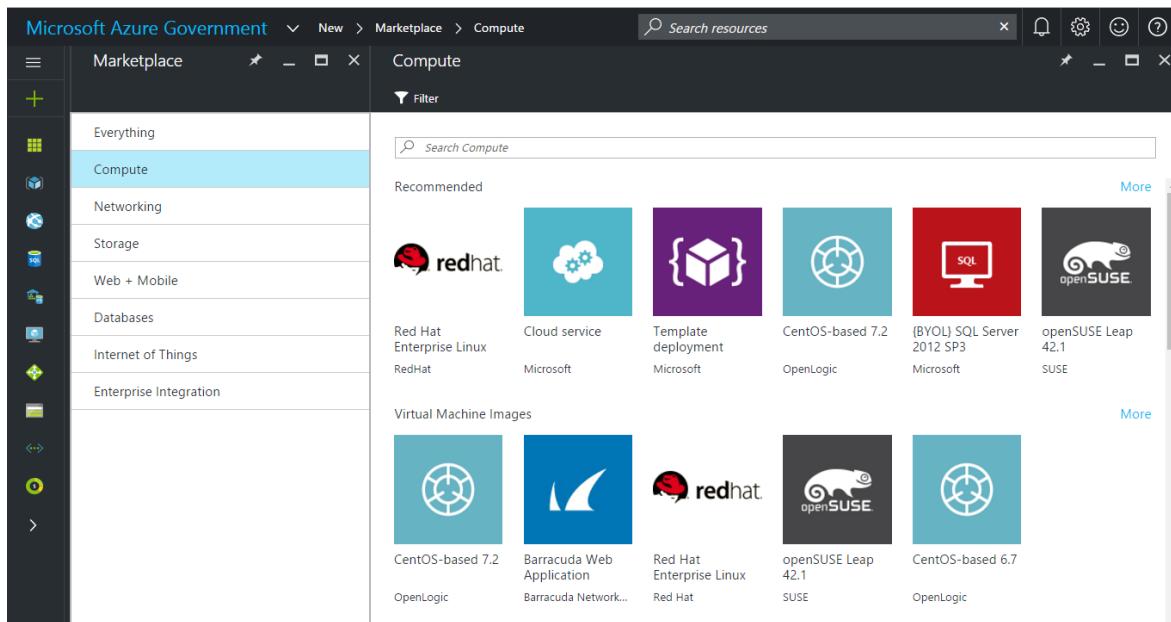
Deploy a Solution to your Subscription

1. Log in to the [Azure Government portal](#).

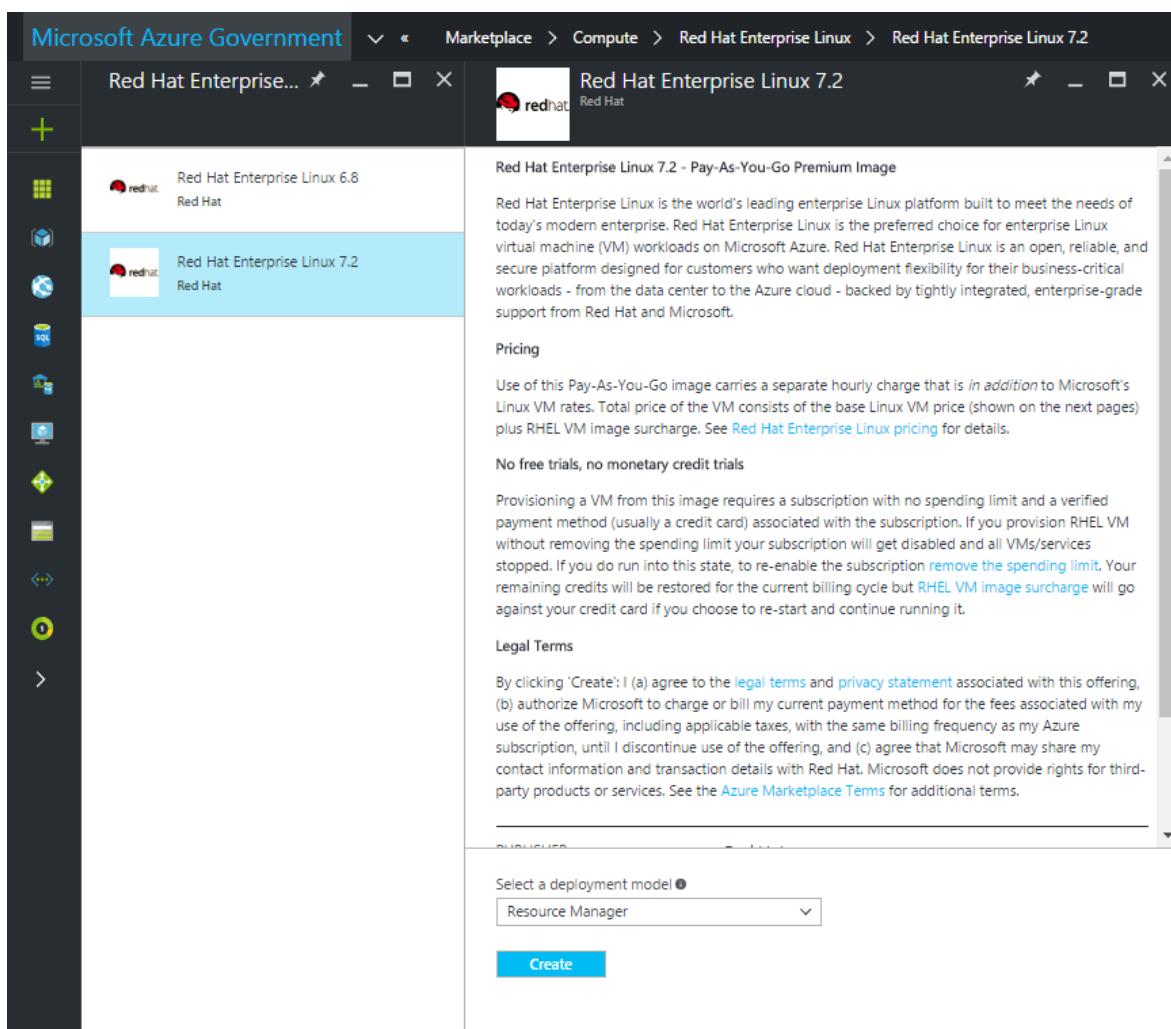
2. Click on +New.



3. Browse through different products to find the right one. The marketplace publisher provides a list of certifications as part of the product description to help you make the right choice.



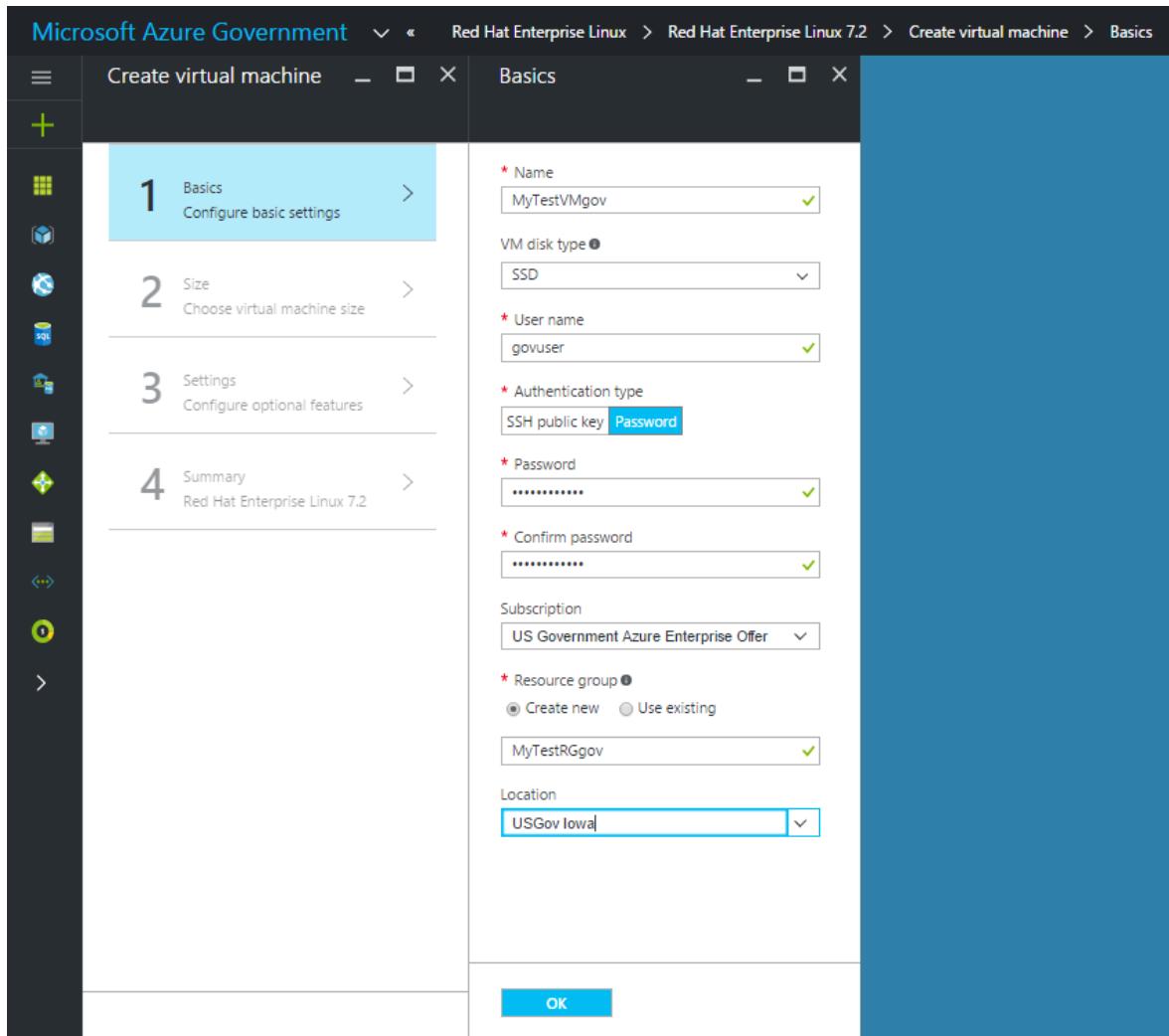
4. Choose a product/image and click **Create**.



5. Enter the required parameters for deployment.

(!) Note

In the Location dropdown, only Azure Government locations are visible



6. To start the provisioning process, click **Ok**.

Next steps

- Subscribe to the [Azure Government blog](#)
- Get help on Stack Overflow by using the [azure-gov](#) tag

Azure Automation in a hybrid environment

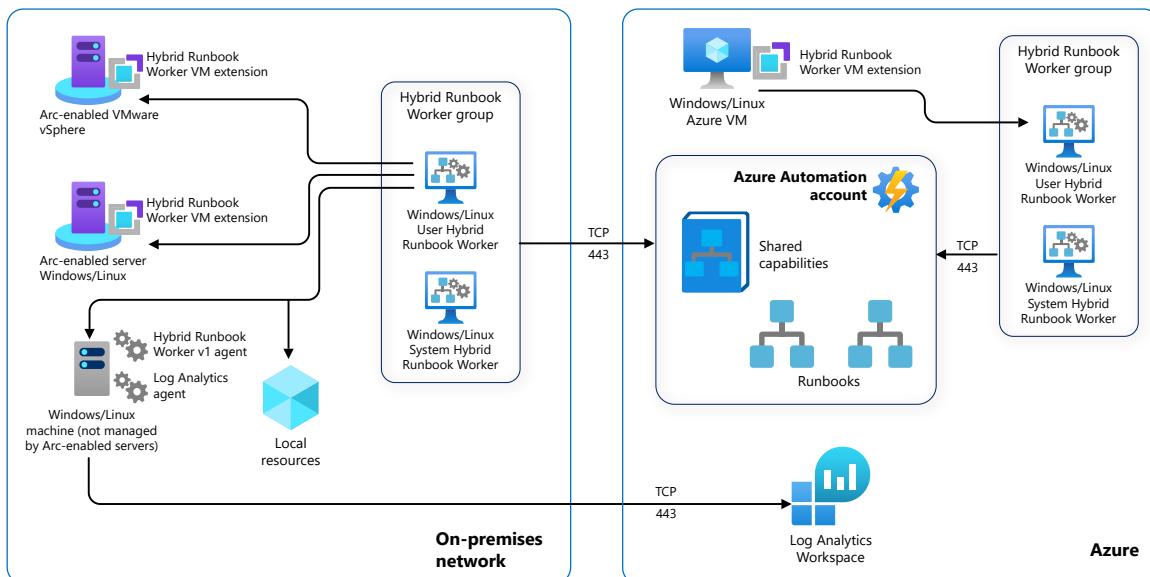
Azure Automation Azure Portal Azure Monitor Azure Virtual Machines Azure Arc

ⓘ Important

Azure Automation Agent-based User Hybrid Runbook Worker (Windows and Linux) will retire on **31 August 2024** and wouldn't be supported after that date. You must complete migrating existing Agent-based User Hybrid Runbook Workers to Extension-based Workers before 31 August 2024. Moreover, starting **1 October 2023**, creating new Agent-based Hybrid Workers wouldn't be possible. [Learn more](#)

Runbooks in Azure Automation run on the Azure cloud platform and might not have access to resources that are in other clouds or in your on-premises environment. You can use the Hybrid Runbook Worker feature of Azure Automation to run runbooks directly on the machine that hosts the role and against resources in the environment to manage those local resources. Runbooks are stored and managed in Azure Automation and then delivered to one or more assigned machines.

Architecture



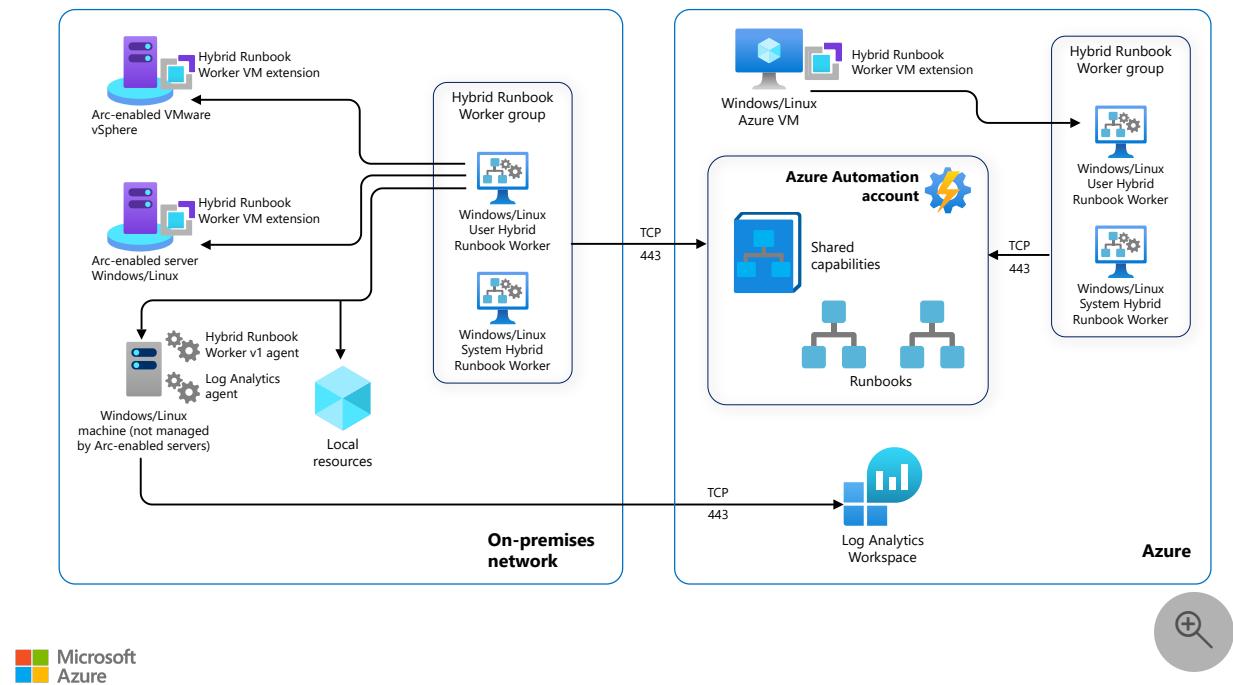
Download a [Visio file](#) of this architecture.

Workflow

The Hybrid Runbook Worker architecture consists of the following:

- **Automation account:** A cloud service that automates configuration and management across your Azure and non-Azure environments.
- **Hybrid Runbook Worker:** A computer that's configured with the Hybrid Runbook Worker feature and can execute runbooks directly on the computer and against the resources in the local environment.
- **Hybrid Runbook Worker group:** Group with multiple Hybrid runbook workers for higher availability and scale to run a set of runbooks.
- **Runbook:** A collection of one or more linked activities that together automate a process or operation. [Learn more](#).
- **On-premises machines and VMs:** Windows or Linux on-premises computers and VMs that are hosted in a private local-area network.
- **Components that are applicable to the extension-based approach (V2):**
 - **Hybrid Runbook Worker VM extension:** A small application that's installed on a computer. The application configures the computer as a Hybrid Runbook Worker.
 - **Arc-enabled server:** Azure Arc-enabled servers make it possible for you to manage Windows and Linux computers and virtual machines that are hosted outside of Azure, whether on your corporate network or on another cloud provider. This management experience is designed to be consistent with how you manage native Azure virtual machines. [Learn more](#).
- **Components that are applicable to the agent-based approach (V1):**
 - **Log Analytics workspace:** A Log Analytics workspace is a data repository for log data that's collected from resources that run in Azure, on-premises, or in another cloud provider.
 - **Automation Hybrid Worker solution:** With this solution, you can create Hybrid Runbook Workers to run Azure Automation runbooks on your Azure and non-Azure computers.

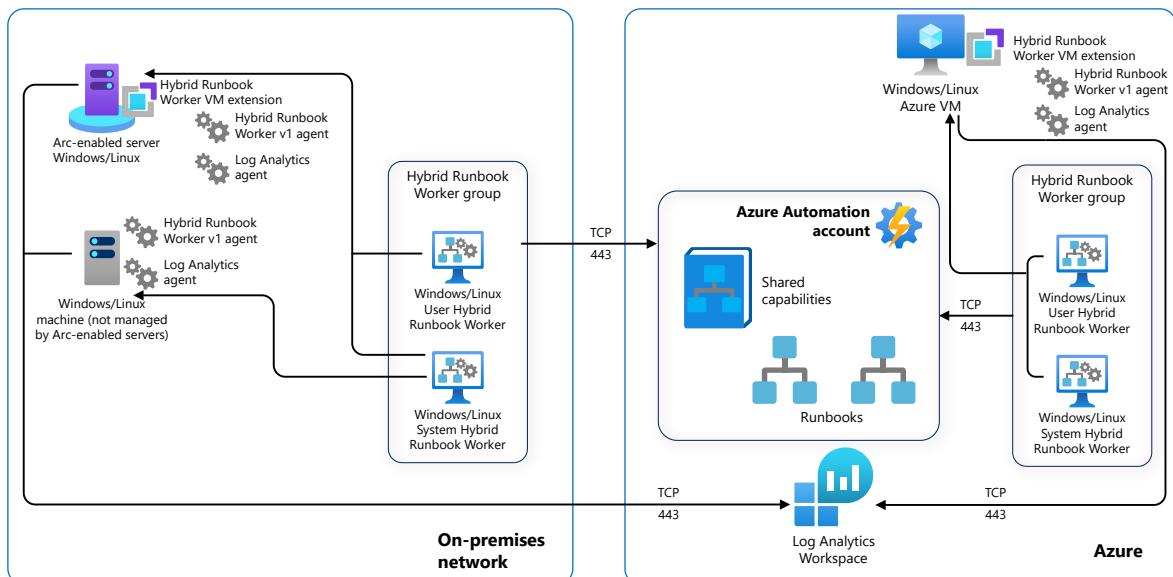
User Hybrid Runbook Worker



Download a [Visio file](#) of this architecture.

Each user Hybrid Runbook Worker is a member of a Hybrid Runbook Worker group that you specify when you install the worker. A group can include a single worker, but you can include multiple workers in a group for high availability. Each machine can host one Hybrid Runbook Worker reporting to one Automation account; you can't register the hybrid worker across multiple Automation accounts. A hybrid worker can only listen for jobs from a single Automation account.

System Hybrid Runbook Worker



Download a [Visio file](#) of this architecture.

Machines that host the system Hybrid Runbook Worker that's managed by Update Management can be added to a Hybrid Runbook Worker group. But you must use the same Automation account for both Update Management and the Hybrid Runbook Worker group membership.

Job execution on Hybrid Runbook Worker

When you start a runbook on a user Hybrid Runbook Worker, you specify the group that it runs on. Each worker in the group polls Azure Automation to see if any jobs are available. If a job is available, the first worker to get the job takes it. The processing time of the jobs queue depends on the hybrid worker hardware profile and load. You can't specify a particular worker. Hybrid worker works on a polling mechanism (every 30 secs) and follows an order of first-come, first-served.

Components

- [Azure Automation](#) is an Azure service for automating cloud management tasks. The **Hybrid Runbook Worker** feature makes it possible to run runbooks on machines that are located in your datacenter in order to manage local resources.
- [Azure Monitor](#) gives you full observability into applications, infrastructure, and network. **Azure Monitor Logs** is a feature of Azure Monitor that collects and organizes log and performance data from monitored resources. **Log Analytics** is a tool in the Azure portal for querying logs and for analyzing the results

Scenario details

Hybrid Runbook Worker installation approach

Azure Automation provides native integration of the Hybrid Runbook Worker role through the Azure virtual machine extension framework. The Azure VM agent is responsible for managing the extension on Azure VMs, both Windows and Linux, and on non-Azure machines through the Arc-enabled servers connected machine agent. There are two Hybrid Runbook Workers installation platforms that are supported by Azure Automation.

[\[\]](#) Expand table

Platform	Description
Extension-based(V2)	Installed by using the Hybrid Runbook Worker VM extension, without any dependency on the reporting activity of the Log Analytics agent that reports to an Azure Monitor Log Analytics workspace. This is the recommended approach , as it offers seamless onboarding and is easy to manage.
Agent-based(V1)	Installed after the Log Analytics agent finishes reporting to an Azure Monitor Log Analytics workspace.

A hybrid worker can co-exist with both platforms: Agent based (V1) and Extension based (V2). If you install Extension based (V2) on a hybrid worker that's already running Agent based (V1), you see two entries of the Hybrid Runbook Worker in the group. One with Platform Extension based (V2) and the other Agent based (V1). [Learn more](#)

Runbook worker types

There are two types of Runbook workers, System and User.

System supports a set of hidden runbooks that are used by the Update Management feature. The runbooks are designed to install user-specified updates on Windows and Linux machines. This type of Hybrid Runbook Worker isn't a member of a Hybrid Runbook Worker group, and therefore doesn't run runbooks that target a Runbook Worker group.

User supports user-defined runbooks that are intended to run directly on the Windows and Linux machines that are members of one or more Runbook Worker groups.

The extension-based Hybrid Runbook Worker only supports the user Hybrid Runbook Worker type and doesn't include the system Hybrid Runbook Worker required for the Update Management feature.

Agent-based (V1) Hybrid Runbook Workers rely on the [Log Analytics agent](#) reporting to an Azure Monitor [Log Analytics workspace](#). The workspace isn't only to collect monitoring data from the machine, but also to download the components that are required to install the agent-based Hybrid Runbook Worker. When Azure Automation [Update Management](#) is enabled, any machine that's connected to your Log Analytics workspace is automatically configured as a system Hybrid Runbook Worker.

Potential use cases

- To execute Azure Automation runbooks directly on an existing Azure virtual machine (VM) or on-premises Arc-enabled server.
- To overcome the Azure Automation sandbox limitation. The common scenarios include executing long-running operations beyond the three-hour limit for cloud jobs, performing resource-intensive automation operations, interacting with local services that run on-premises or in hybrid environments, running scripts that require elevated permissions, and so on.
- To overcome organizational restrictions on keeping data in Azure for governance and security reasons. Even though you can't execute Automation jobs in the cloud, you can run them on an on-premises machine that's onboarded as a Hybrid Runbook Worker.
- To automate operations on multiple non-Azure resources that run in on-premises, hybrid, or multicloud environments. You can onboard one of those machines as a Hybrid Runbook Worker and target automation on the remaining on-premises machines.
- To access other services privately from the Azure Virtual Network (VNet) without having to open an outbound connection to the internet, you can execute runbooks on a Hybrid Worker connected to the Azure virtual network.

Considerations

These considerations implement the pillars of the Azure Well-Architected Framework, which is a set of guiding tenets that can be used to improve the quality of a workload. For more information, see [Microsoft Azure Well-Architected Framework](#).

Reliability

Reliability ensures that your application can meet the commitments that you make to your customers. For more information, see [Overview of the reliability pillar](#).

- A Hybrid Runbook Worker Group with more than one machine configured with the Hybrid Worker Role provides high availability because runbooks will start only on servers that are running and healthy.
- The extension-based (V1) Hybrid Runbook Worker only supports the User Hybrid Runbook Worker type and doesn't include the System Hybrid Runbook Worker that's required for the Update Management feature.
- The following applies only to the agent-based approach (V1). Currently, mappings between a Log Analytics Workspace and an Automation account are supported in several regions. For more information, see [Supported regions for linked Log Analytics workspace](#).

Security

Security provides assurances against deliberate attacks and the abuse of your valuable data and systems. For more information, see [Overview of the security pillar](#).

- **Encryption of sensitive assets in Automation:** An Azure Automation Account can contain sensitive assets such as credentials, certificate, connection, and encrypted variables that might be used by the runbooks. Each secure asset is encrypted by default by using a Data Encryption key that's generated for each Automation Account. These keys are encrypted and stored in Azure Automation with an Account Encryption Key (AEK) that can be stored in the Key vault for customers who want to manage encryption with their own keys. By default, AEK is encrypted by using Microsoft-managed keys. Use the following guidelines to [apply encryption of secure assets in Azure Automation](#).
- **Runbook permission:** By default, runbook permissions for a Hybrid Runbook Worker run in a system context on the machine where they're deployed. A runbook provides its own authentication to local resources. Authentication can be configured by using managed identities for Azure resources or by specifying a Run As account to provide a user context for all runbooks.
- **Network planning:**
 - If you use a proxy server for communication between Azure Automation and the machines that run the Hybrid Runbook Worker, ensure that the appropriate resources are accessible. The timeout for requests from the Hybrid Runbook Worker and Automation services is 30 seconds. After three attempts, the request fails.
 - Hybrid Runbook Worker requires outbound internet access over TCP port 443 to communicate with Automation. If you use a firewall to restrict access to the Internet, you must configure the firewall to permit access. For agent-based (V1) computers with restricted internet access, use Log Analytics gateway to configure communication with Azure Automation and Azure Log Analytics Workspace.
 - There is a CPU quota limit of 5% while configuring extension-based Linux Hybrid Runbook worker. There is no such limit for Windows extension-based Hybrid Runbook Worker.
- **Azure security baseline for Automation:** [The Azure security baseline for Automation](#) contains recommendations on how to improve your security configuration to protect your assets by following the best-practice guidance.

Cost optimization

Cost optimization is about looking at ways to reduce unnecessary expenses and to improve operational efficiencies. For more information, see [Overview of the cost optimization pillar](#).

- Azure Automation costs are priced for job execution per minute. Every month, the first 500 minutes of process automation are free. Use the [Azure pricing calculator](#) to estimate costs. For more information about the Azure Automation pricing models, see [Automation pricing](#).
- For the agent-based approach (V1), Azure Log Analytics Workspace might generate additional costs that are related to the amount of log data that's stored in Azure Log Analytics. The pricing model is based on consumption. The costs are associated for data ingestion and data retention. For ingesting data into Azure Log Analytics, use Capacity Reservation or the Pay-As-You-Go model that includes 5 gigabytes (GB) free per billing account per month. Data retention for the first 31 days is free of charge. For the pricing models for Log Analytics, see [Azure Monitor pricing](#).

Operational excellence

Operational excellence covers the operations processes that deploy an application and keep it running in production. For more information, see [Overview of the operational excellence pillar](#).

Manageability

- The extension-based approach (V2) offers ease of manageability as compared to agent-based approach (V1) through:
 - Native integration with ARM identity for Hybrid Runbook Worker and provides the flexibility for governance at scale through policies and templates.
 - Centralized control and management of identities and resource credentials, since it uses VM system-assigned identities that are provided by Microsoft Entra ID.
 - Unified experience for both Azure and non-Azure machines while onboarding and deboarding Hybrid Runbook Workers.
- Applicable only for agent-based approach (V1):
 - To accelerate deployment of the Log Analytics Agent with Hybrid Worker Role running on Windows machine, use the PowerShell script [New-OnPremiseHybridWorker.ps1](#)
 - Deployment of many agents in on-premises infrastructure can be orchestrated by using command line scripts and deployed by using Group Policy or System Center Configuration Manager.

DevOps

- Azure Automation allows integration with popular source control systems, Azure DevOps and GitHub. With source control, you can integrate the existing development environment that contains your scripts and custom code that have been previously tested in an isolated environment.
- For information on how to integrate Azure Automation with your source control environment, see [Use source control integration](#).

Contributors

This article is maintained by Microsoft. It was originally written by the following contributors.

Principal author:

- [Mike Martin](#) | Senior Cloud Solution Architect

To see non-public LinkedIn profiles, sign in to LinkedIn.

Next steps

More about Azure Automation:

- [Hybrid Runbook Worker overview](#)
- [Deploy extension-based Windows or Linux User Hybrid Runbook Worker](#)
- [Deploy an agent-based Windows Hybrid Runbook Worker in Automation](#)
- [Deploy an agent-based Linux Hybrid Runbook Worker in Automation](#)
- [Create an Azure Automation account](#)
- [Create a runbook in Azure Automation using Managed Identities](#)
- [Run Automation runbooks on a Hybrid Runbook Worker](#)
- [Pre-requisites: Azure Automation network configuration details](#)
- [Azure Arc Overview](#)
- [What is Azure Arc enabled servers?](#)

More about Azure Monitor and Monitor Logs:

- [Azure Monitor Logs overview](#)
- [Overview of Log Analytics in Azure Monitor](#)

Related resources

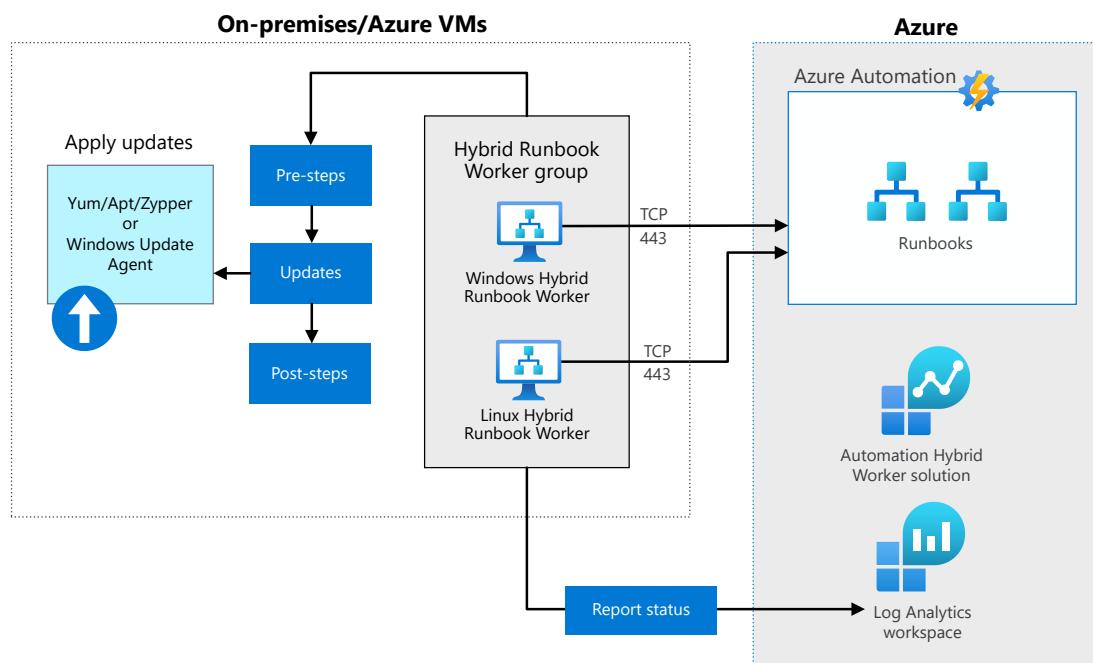
- Hybrid architecture design
- Connect an on-premises network to Azure
- Enterprise monitoring with Azure Monitor
- Computer forensics chain of custody in Azure
- Disaster Recovery for Azure Stack Hub virtual machines

Azure Automation update management

Azure Automation Azure Log Analytics Azure Monitor Azure Resource Manager Azure Virtual Machines

This reference architecture illustrates how to design a hybrid update management solution to manage updates on both Microsoft Azure and on-premises Windows and Linux computers.

Architecture



Download a [Visio file](#) of this architecture.

Workflow

The architecture consists of the following services:

- **Log Analytics workspace:** A [Log Analytics workspace](#) is a data repository for log data that's collected from resources that run in Azure, on-premises, or in another cloud provider.

- **Automation Hybrid Worker solution:** Create [Hybrid Runbook Workers](#) to run [Azure Automation](#) runbooks on your Azure and non-Azure computers.
- **Automation account:** This is a cloud service that automates configuration and management across your Azure and non-Azure environments.
- **Hybrid Runbook Worker:** This is a computer that's configured with the Hybrid Runbook Worker feature and can run runbooks directly on the computer and against the resources in the local environment.
- **Hybrid Runbook Worker group:** It's a group of Hybrid Runbook Workers used for high availability.
- **Runbook:** This is a collection of one or more linked activities that together automate a process or operation.
- **On-premises computers and VMs:** These are on-premises computers and VMs with Windows or Linux operating systems that reside on-premises.
- **Azure VMs:** Azure VMs include Windows or Linux VMs that are hosted in Azure.

Components

- [Azure Automation](#) ↗
- [Azure Virtual Machines](#) ↗
- [Azure Monitor](#) ↗
- [Azure Arc](#) ↗

Scenario details

Typical uses for this architecture include:

- Managing updates across on-premises and in Azure using the Update Management component of Automation Account.
- Using scheduled deployments to orchestrate the installation of updates within a defined maintenance window.

Recommendations

The following recommendations apply for most scenarios. Follow them unless you have a specific requirement that overrides them.

Update Management

[Update Management](#) is a configuration component of Automation. Windows and Linux computers, both in Azure and on-premises, send assessment information about missing

updates to the Log Analytics workspace. Azure Automation then uses that information to create a schedule for automatic deployment of the missing updates.

The following steps highlight the actual implementation:

1. Create a Log Analytics workspace.
2. Create an Automation account.
3. Link the Automation account with the Log Analytics workspace.
4. Enable Update Management for Azure VMs.
5. Enable Update Management for non-Azure VMs.

Create a Log Analytics workspace

Before you create a Log Analytics workspace, ensure that you have at least Log Analytics Contributor role permissions.

You can have more than one Log Analytics workspace for data isolation or for geographic location of data storage, but the Log Analytics agent can be configured to report to one Log Analytics workspace. For more information, review the [Designing your Azure Monitor Logs deployment](#) before you create the workspace.

Use the following procedure to create a Log Analytics workspace:

1. Sign in to the Azure portal at <https://portal.azure.com>.
2. In the Azure portal, select **Create a resource**.
3. In the **Search the Marketplace** box, enter **Log Analytics**. As you begin entering this text, the list filters based on your input. Select **Log Analytics workspaces**.
4. Select **Create**, and then configure the following items:
 - a. Select a different **Subscription** in the drop-down list if the default selection isn't appropriate.
 - b. For the **Resource Group**, choose to use an existing resource group that's already set up or create a new one.
 - c. Provide a unique name for the new **Log Analytics workspace**, such as *HybridWorkspace-yourname*
 - d. Select the **Location** for your deployment.
 - e. Select **pricing tier** to proceed to further customizations.
 - f. If you're creating a workspace in a subscription that was created after April 2, 2018, it'll automatically use the **Per GB** pricing plan, and the option to select a pricing tier won't be available. If you're creating a workspace for an existing subscription that was created before that date or for a subscription that was tied to an existing Enterprise Agreement enrollment, select your preferred

pricing tier. For more information about the particular tiers, refer to [Log Analytics Pricing details](#).

- g. Select **Tags** and optionally provide a name and value for categorization of the resources.
 - h. Select **Review + Create**.
5. After providing the required information in the **Log Analytics workspace** pane, select **Create**.

Create an Automation account

After the Automation Hybrid Worker solution has been added to the Log Analytics workspace, proceed with creation of the Automation account. Refer to [Supported regions for linked Log Analytics workspace](#) to select the regions for Automation account and Log Analytics workspace. It's important that you create the Automation account based on the region mapping document and preferably in the same resource group as the Log Analytics workspace.

Use the following procedure to create an Automation account:

1. In the Azure portal, select **Create a resource**.
2. In the **Search the Marketplace** box, enter **Automation**. As you begin entering this text, the list filters based on your input. Select **Automation**, and then select **Create**.
3. Select **Create**, and then configure the following items:
 - a. Provide the **Name** for the Automation account, such as *hybrid-auto*.
 - b. Select a different **Subscription** in the drop-down list if the default selection isn't appropriate.
 - c. For the **Resource Group**, choose the same resource group in which you want to create the automation account.
 - d. Select the **Location** based on the region mapping document.
 - e. **Create Azure Run As account** is optional because this only provides authentication with Azure to manage Azure resources from Automation runbooks.
4. After providing the required information in the **Add Automation Account** pane, select **Create**.

Link the Automation account with the Log Analytics workspace

Automation accounts use the Hybrid Runbook Worker components that deploy in the Log Analytics workspace. You must integrate those services before you deploy a Log Analytics agent on an on-premises computer. Currently, mappings between Log

Analytics workspaces and Automation accounts are supported in several regions. For further information, refer to [Supported regions for linked Log Analytics workspace](#).

Use the following procedure to link an Automation account with a Log Analytics workspace:

1. In the Azure portal, select **All services**, and then enter **automation**. As you begin entering this text, the list filters based on your input. Select **Automation Account**, and then select the Automation account that you created earlier.
2. In the **Automation Account** pane, select **Update Management** in the **Update Management** section.
3. In the **Update Management** pane, configure the following items:
 - a. Select a different **Subscription** in the drop-down list if the default selection isn't appropriate.
 - b. For **Log Analytics workspace**, select your existing Log Analytics workspace; for example, *HybridWorkspace-yourname*.
4. After providing the required information in the **Update Management** pane, select **Enable**.

Enable Update Management for Azure VMs

Enable Update Management for Azure VMs by using the following tools:

- [Azure Resource Manager template](#). Microsoft provides a sample template that can automate creation of an Azure Log Analytics workspace, creation of an Automation account, linking the Automation account to the Log Analytics workspace, and enabling Update Management.
- [Update Management from the Azure portal](#). Use this method when you want to update multiple VMs that reside in different regions.
- [Update Management from an Azure VM](#). This will configure updates for a selected VM.
- [Update Management from an Automation account](#). Use this method when you want to update both Azure and non-Azure computers and VMs at the same time.
- [Update Management from a runbook](#). Use this method to enable Update Management as an automated procedure combined with other automation activities.

Use the following procedure to enable Update Management for Azure VMs:

1. In the Azure portal, select **All services**, and then enter **automation**. As you begin entering this text, the list filters based on your input. Select **Automation Account**, and then select the Automation account that you created earlier.

2. In the **Automation Account** pane, select **Update Management** in the **Update Management** section.
3. In the **Update Management** pane, select **Add Azure VMs**, select one or more VMs that are ready for Update Management, and then select **Enable**.

Deploy the Log Analytics agent and connect to a Log Analytics workspace

Deploying a Hybrid Runbook Worker component is part of the deployment of a Log Analytics agent.

If you test the solution by using an Azure VM, you can install the Log Analytics agent and enroll the VM in an existing Log Analytics workspace by using a VM extension for both [Linux](#) and [Windows](#). You can also deploy the agent by using Azure Automation Desired State Configuration, a Windows PowerShell script, or by using a Resource Manager template for VMs. For more information, refer to [Connect Windows computers to Azure Monitor](#).

For non-Azure VMs, deploy the agent by using a manual or automated process both on physical Windows and Linux computers or VMs that are in your environment.

For Windows computers, configure the agent to communicate with the Log Analytics service by using the Transport Layer Security (TLS) 1.2 protocol. Refer to [Connect Windows computers to Azure Monitor](#) for a detailed explanation of the deployment procedure.

The Log Analytics agent for Linux can be deployed:

- [Manually](#) by using a shell script bundle that contains Debian and Red Hat Package Manager (RPM) packages for each of the agent components. This is recommended when a Linux computer doesn't have internet connectivity and will communicate with the Log Analytics service through the [Log Analytics gateway](#).
- By using a [wrapper-script](#) that's hosted on GitHub when the computer has connectivity to the internet.

The Log Analytics agent must be configured to communicate with a Log Analytics workspace by using the [workspace ID and key](#) of the Log Analytics workspace.

Use the following procedure to deploy a Log Analytics agent and connect to a Log Analytics workspace:

1. In the Azure portal, search for and select **Log Analytics workspaces**.

2. In your list of Log Analytics workspaces, select the workspace that the agent uses for reporting.
3. Select **Agents management**.
4. Copy and paste the **Workspace ID** and **Primary Key** into your favorite editor.
5. In your Log Analytics workspace, from the **Windows Servers** page that you browsed to earlier, select the appropriate **Download Windows Agent** version to download based on the processor architecture of the Windows operating system.
6. Run **Setup** to install the agent on your computer.
7. On the **Welcome** page, select **Next**.
8. On the **License Terms** page, read the license, and then select **I Agree**.
9. On the **Destination Folder** page, change or keep the default installation folder, and then select **Next**.
10. On the **Agent Setup Options** page, choose to connect the agent to Azure Log Analytics, and then select **Next**.
11. On the **Azure Log Analytics** page, perform the following steps:
 - a. Paste the **Workspace ID** and **Workspace Key (Primary Key)** that you copied earlier. If the computer reports to a Log Analytics workspace in a Microsoft Azure Government cloud, select **Azure US Government** in the **Azure Cloud** drop-down list.
 - b. If the computer needs to communicate through a proxy server to the Log Analytics service, select **Advanced**, and then provide the URL and port number of the proxy server. If your proxy server requires authentication, enter the username and password to authenticate with the proxy server, and then select **Next**.
12. Select **Next** after you finish providing the necessary configuration settings.

Enable Update Management for non-Azure computers

Enabling Update Management on non-Azure computers has the following prerequisites:

- Deploy the Log Analytics agent and connect to a Log Analytics workspace.

Previous procedures explain how to configure those prerequisites.

After installing the Log Analytics agent on an on-premises computer, enable Update Management in the Azure portal by using the following procedure:

1. In the Azure portal, select **All services**, and then enter **automation**. As you begin entering this text, the list filters based on your input. Select **Automation Account**, and then select the Automation account that you created earlier.
2. In the **Automation Account** pane, select **Update Management** in the **Update Management** section.

3. In the **Update Management** pane, select **Manage machines**, and then select computers that are listed and have been configured to send log data to the Log Analytics workspace.
4. Select **Enable** to finish the configuration of Update Management on non-Azure machines.

Each Windows computer managed by Update Management is listed in the **Hybrid Worker groups** pane as a System Hybrid Worker group for the Automation account. Use these groups only for deploying updates, not for targeting the groups with runbooks for automated tasks.

Considerations

These considerations implement the pillars of the Azure Well-Architected Framework, which is a set of guiding tenets that can be used to improve the quality of a workload. For more information, see [Microsoft Azure Well-Architected Framework](#).

Manageability

Manage updates for Azure VMs and non-Azure machines

Update assessment for all missing updates that both Azure VMs and non-Azure computers require is visible in the **Update Management** section of your Automation account.

Schedule an update deployment by using the Azure portal or by using PowerShell, which creates schedule assets that are linked to the **Patch-MicrosoftOMSComputers** runbook.

Use the following procedure to schedule a new update deployment:

1. In your Automation account, go to **Update management** under **Update management**, and then select **Schedule update deployment**.
2. Under **New update deployment**, use the **Name** box to enter a unique name for your deployment.
3. Select the operating system to target for the update deployment.
4. In the **Groups to update** pane, define a query that combines subscription, resource groups, locations, and tags to build a dynamic group of Azure VMs to include in

your deployment. To learn more, refer to [Use dynamic groups with Update Management](#).

5. In the **Machines to update** pane, select a saved search, an imported group, or pick **Machines** from the drop-down menu, and then select individual machines.
6. Use the **Update classifications** drop-down menu to specify [update classifications](#) for products.
7. Use the **Include/exclude updates** pane to select specific updates for deployment.
8. Select **Schedule settings** to define a time when the update deployment will run on computers.
9. Use the **Recurrence** box to specify if the deployment occurs once or uses a recurring schedule, and then select **OK**.
10. In the **Pre-scripts + Post-scripts (Preview)** region, select the scripts to run before and after your deployment. To learn more, refer to [Manage pre-scripts and post-scripts](#).
11. Use the **Maintenance window (minutes)** box to specify the amount of time that's allowed for updates to install.
12. Use the **Reboot options** box to specify the way to handle reboots during deployment.
13. When you finish configuring the deployment schedule, select **Create**.

Results of a completed update deployment are visible in the **Update Management** pane on the **History** tab.

Configure Windows Update settings

Azure Update Management depends on Windows Update Client to download and install updates either from Windows Update (default setting) or from Windows Server Update Server. Configure Windows Update Client settings to connect to Windows Server Update Services (WSUS) by using:

- Local Group Policy Editor
- Group Policy
- PowerShell
- Directly editing the registry

For more information, refer to how to [configure Windows Update settings](#).

Integrate Update Management with Microsoft Endpoint Configuration Manager

The Software Update Management cycle can integrate with Microsoft Endpoint Configuration Manager for customers that are already using this product to manage PCs, servers, and mobile devices.

To integrate Software Update Management with Endpoint Configuration Manager, first integrate Endpoint Configuration Manager with Azure Monitor logs and import the collections in the Log Analytics workspace.

For details, refer to [Connect Configuration Manager to Azure Monitor](#).

To manage updates on local computers, configure them with:

- The Endpoint Configuration Manager client.
- The Log Analytics agent, which is configured to report to a Log Analytics workspace that's enabled for Update Management.
- Windows agents that are configured to communicate with WSUS or have access to Microsoft Update.

To manage updates on computers with Endpoint Configuration Manager, deploy the following roles on the Endpoint Configuration Manager computer:

- Management point. This site system role manages clients with a policy that contains configuration settings and service location information.
- Distribution point. This contains source files for clients.
- Software update point. This is a role on the server that's hosting WSUS.

Manage software updates by using:

- Endpoint Configuration Manager
- Azure Automation

Partner updates on Windows machines can be deployed from a custom repository that [System Center Updates Publisher](#) (SCUP) provides. SCUP can import custom updates either in standalone WSUS or integrated with Endpoint Configuration Manager.

For more information, refer to [Integrate Update Management with Windows Endpoint Configuration Manager](#).

Deploy the Log Analytics agent by using a PowerShell script

To accelerate deployment of the Log Analytics agent with the Hybrid Worker role running on a Windows computer, use the `New-OnPremiseHybridWorker.ps1` PowerShell script. The script:

- Installs the necessary modules.
- Signs in with your Azure account.
- Verifies the existence of a specified resource group and Automation account.
- Creates references to Automation account attributes.
- Creates an Azure Monitor Log Analytics workspace if not specified.
- Enables the Automation solution in the workspace.
- Downloads and installs the Log Analytics agent for the Windows operating system.
- Registers the machine as a Hybrid Runbook Worker.

Deploying many agents in an on-premises infrastructure can be orchestrated by using command-line scripts and by using Group Policy or Endpoint Configuration Manager.

Use dynamic groups for Azure and non-Azure machines

Dynamic groups for Azure VMs filter VMs based on a combination of:

- Subscriptions
- Resource groups
- Locations
- Tags

Dynamic groups for non-Azure computers use saved searches to filter the computers for deployment of the update. Saved searches, also known as *computer groups*, can be created by using:

- A log query. Use Azure Data Explorer to define a logical expression to filter the computers.
- Active Directory Domain Services. A group is created in Log Analytics workspace for any members of an Active Directory domain.
- Endpoint Configuration Manager. Import computer collections from Endpoint Configuration Manager into a Log Analytics workspace.
- WSUS. Groups that are created in WSUS servers can be imported into a Log Analytics workspace.

For more information on how to create computer groups for filtering machines for update deployment, refer to [Computer groups in Azure Monitor log queries](#).

Scalability

Azure Automation can process up to 1,000 computers per update deployment. If you expect to update more than 1,000 computers, you can split up the updates among multiple update schedules. Refer to [Azure subscription and service limits, quotas, and constraints](#).

Availability

- Currently, mappings between Log Analytics Workspace and Automation Account are supported in several regions. For further information, refer to [Supported regions for linked Log Analytics workspace](#).
- Supported client types: Update assessment and patching is supported on Windows and Linux computers that run in Azure or in your on-premises environment. Currently, the Windows client isn't officially supported. For a list of the supported clients, refer to [Supported client types](#).

Security

Security provides assurances against deliberate attacks and the abuse of your valuable data and systems. For more information, see [Overview of the security pillar](#).

- Update Management permissions: The Update Management component of Automation and the Log Analytics workspace component of Monitor can use Azure role-based access control (Azure RBAC) with built-in roles from Azure Resource Manager. For segregation of the duties, these roles can be assigned to different users, groups, and security principals. For a list of the roles in Automation accounts, refer to [Manage role permissions and security](#).
- Encryption of sensitive assets in Automation: An Automation account can contain sensitive assets such as credentials, certificates, and encrypted variables that runbooks might use. Each secure asset is encrypted by default using a data encryption key that's generated for each Automation account. These keys are encrypted and stored in Automation with an account encryption key that can be stored in the Azure Key Vault for customers who want to manage encryption with their own keys. By default, an account encryption key is encrypted by using Microsoft-managed keys. Use the following guidelines to [apply encryption of secure assets in Azure Automation](#).
- Runbook permissions for a Hybrid Runbook Worker: By default, runbook permissions for a Hybrid Runbook Worker run in a system context on the machine where they're deployed. A runbook provides its own authentication to local resources. Authentication can be configured using managed identities for Azure resources or by specifying a Run As account to provide a user context for all runbooks.

- Network planning: Hybrid Runbook Worker requires outbound internet access over TCP port 443 to communicate with Automation. For computers with restricted internet access, you can use the [Log Analytics gateway](#) to configure communication with Automation and an Azure Log Analytics workspace.
- Azure Security baseline for Automation: [Azure security baseline for Automation](#) contains recommendations about how to increase overall security to protect your assets following best practice guidance.

DevOps

- You can schedule update deployment programmatically through the REST API. For more information, refer to [Software Update Configurations - Create](#).
- Azure Automation allows integration with popular source control systems like Azure DevOps and GitHub. With source control, you can integrate an existing development environment that contains your scripts and custom code that has been previously tested in an isolated environment.
- For more information about how to integrate Automation with your source control environment, refer to [Use source control integration](#).

Cost optimization

Cost optimization is about looking at ways to reduce unnecessary expenses and improve operational efficiencies. For more information, see [Overview of the cost optimization pillar](#).

- Use the [Azure pricing calculator](#) to estimate costs. For more information about Automation pricing models, refer to [Automation pricing](#).
- Azure Automation costs are priced for job execution per minute or for configuration management per node. Every month, the first 500 minutes of process automation and configuration management on five nodes are free.
- An Azure Log Analytics workspace might generate more costs related to the amount of log data that's stored in Azure Log Analytics. The pricing is based on consumption, and the costs are associated with data ingestion and data retention. For ingesting data into Azure Log Analytics, use the capacity reservation or pay-as-you-go model that includes 5 gigabytes (GB) free a month for each billing account. Data retention for the first 31 days is free of charge.
- Use the Azure pricing calculator to estimate costs. For more information about Log Analytics pricing models, refer to [Azure Monitor pricing](#).

Contributors

This article is maintained by Microsoft. It was originally written by the following contributors.

Principal author:

- [Mike Martin](#) | Senior Cloud Solution Architect

To see non-public LinkedIn profiles, sign in to LinkedIn.

Next steps

More about Azure Automation:

- [Hybrid Runbook Worker overview](#)
- [Create an Azure Automation account](#)
- [Pre-requisites: Azure Automation network configuration details](#)
- [Azure Automation Update Management](#)
- [Overview of Log Analytics in Azure Monitor](#)
- [Overview of VM insights](#)
- [Azure Arc Overview](#)
- [What is Azure Arc enabled servers?](#)

Related resources

- [Azure Automation in a hybrid environment](#)
- [Event-based cloud automation](#)
- [Azure Automation State Configuration](#)

Azure Virtual Desktop for the enterprise

Microsoft Entra ID

Microsoft Entra

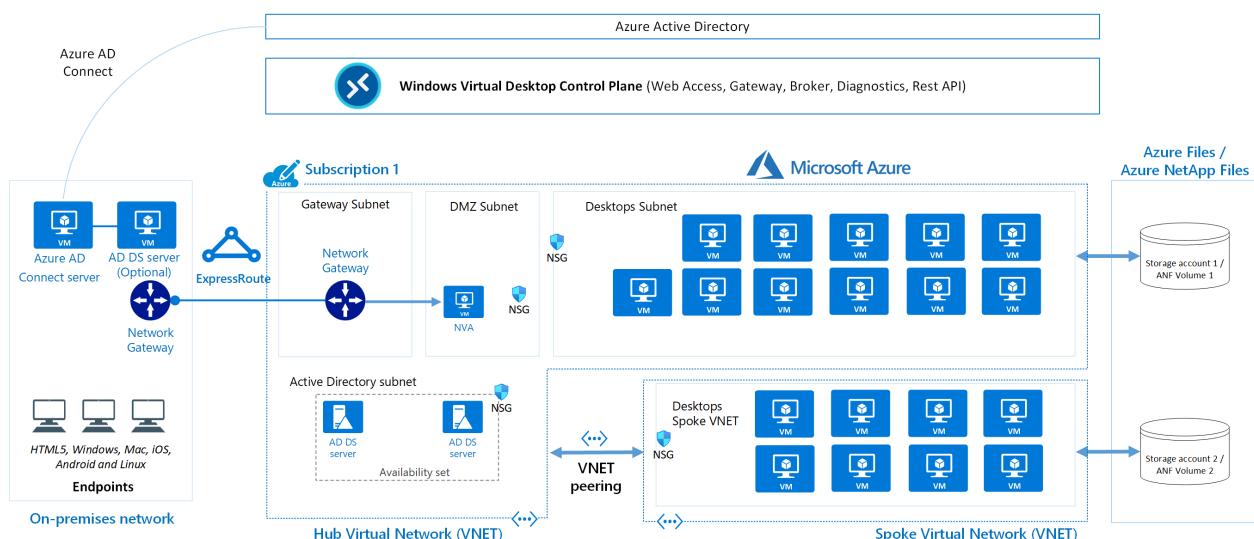
Azure Virtual Network

Azure Virtual Desktop

Azure Virtual Desktop [↗](#) is a desktop and application virtualization service that runs in Azure. This article is intended to help desktop infrastructure architects, cloud architects, desktop administrators, and system administrators explore Azure Virtual Desktop and build virtualized desktop infrastructure (VDI) solutions at enterprise scale. Enterprise-scale solutions generally cover 1,000 or more virtual desktops.

Architecture

A typical architectural setup for Azure Virtual Desktop is illustrated in the following diagram:



Download a [Visio file ↗](#) of this architecture.

Dataflow

The diagram's dataflow elements are described here:

- The application endpoints are in a customer's on-premises network. Azure ExpressRoute extends the on-premises network into Azure, and Microsoft Entra Connect integrates the customer's Active Directory Domain Services (AD DS) with Microsoft Entra ID.

- The Azure Virtual Desktop control plane handles web access, gateway, broker, diagnostics, and extensibility components such as REST APIs.
- The customer manages AD DS and Microsoft Entra ID, Azure subscriptions, virtual networks, [Azure Files or Azure NetApp Files](#), and the Azure Virtual Desktop host pools and workspaces.
- To increase capacity, the customer uses two Azure subscriptions in a hub-spoke architecture and connects them via virtual network peering.

For more information about FSLogix Profile Container - Azure Files and Azure NetApp Files best practices, see [FSLogix configuration examples](#).

Components

Azure Virtual Desktop service architecture is similar to [Windows Server Remote Desktop Services](#). Although Microsoft manages the infrastructure and brokering components, enterprise customers manage their own desktop host virtual machines (VMs), data, and clients.

Components that Microsoft manages

Microsoft manages the following Azure Virtual Desktop services, as part of Azure:

- **Web Access:** By using the [Web Access](#) service within Azure Virtual Desktop you can access virtual desktops and remote apps through an HTML5-compatible web browser just as you would with a local PC, from anywhere and on any device. You can secure web access by using multifactor authentication in Microsoft Entra ID.
- **Gateway:** The Remote Connection Gateway service connects remote users to Azure Virtual Desktop apps and desktops from any internet-connected device that can run an Azure Virtual Desktop client. The client connects to a gateway, which then orchestrates a connection from a VM back to the same gateway.
- **Connection Broker:** The Connection Broker service manages user connections to virtual desktops and remote apps. Connection Broker provides load balancing and reconnection to existing sessions.
- **Diagnostics:** Remote Desktop Diagnostics is an event-based aggregator that marks each user or administrator action on the Azure Virtual Desktop deployment as a success or failure. Administrators can query the event aggregation to identify failing components.

- **Extensibility components:** Azure Virtual Desktop includes several extensibility components. You can manage Azure Virtual Desktop by using Windows PowerShell or with the provided REST APIs, which also enable support from third-party tools.

Components that you manage

You manage the following components of Azure Virtual Desktop solutions:

- **Azure Virtual Network:** With [Azure Virtual Network](#), Azure resources such as VMs can communicate privately with each other and with the internet. By connecting Azure Virtual Desktop host pools to an Active Directory domain, you can define network topology to access virtual desktops and virtual apps from the intranet or internet, based on organizational policy. You can connect an Azure Virtual Desktop instance to an on-premises network by using a virtual private network (VPN), or you can use [Azure ExpressRoute](#) to extend the on-premises network into Azure over a private connection.
- **Microsoft Entra ID:** Azure Virtual Desktop uses [Microsoft Entra ID](#) for identity and access management. Microsoft Entra integration applies Microsoft Entra security features, such as conditional access, multifactor authentication, and [Intelligent Security Graph](#), and it helps maintain app compatibility in domain-joined VMs.
- **Active Directory Domain Services (Optional):** Azure Virtual Desktop VMs can either be domain joined to an [AD DS](#) service or use [Deploy Microsoft Entra joined virtual machines in Azure Virtual Desktop](#)
 - When using an AD DS domain, the domain must be in sync with Microsoft Entra ID to associate users between the two services. You can use [Microsoft Entra Connect](#) to associate AD DS with Microsoft Entra ID.
 - When using Microsoft Entra join, review the [supported configurations](#) to ensure your scenario is supported.
- **Azure Virtual Desktop session hosts:** Session hosts are VMs that users connect to for their desktops and applications. Several versions of Windows are supported and you can create images with your applications and customizations. You can choose VM sizes, including GPU-enabled VMs. Each session host has an Azure Virtual Desktop host agent, which registers the VM as part of the Azure Virtual Desktop workspace or tenant. Each host pool can have one or more app groups, which are collections of remote applications or desktop sessions that you can access. To see which versions of Windows are supported, see [Operating systems and licenses](#).

- **Azure Virtual Desktop workspace:** The Azure Virtual Desktop workspace or tenant is a management construct for managing and publishing host pool resources.

Scenario details

Potential use cases

The greatest demand for enterprise virtual desktop solutions comes from:

- Security and regulation applications, such as financial services, healthcare, and government.
- Elastic workforce needs, such as remote work, mergers and acquisitions, short-term employees, contractors, and partner access.
- Specific employees, such as bring your own device (BYOD) and mobile users, call centers, and branch workers.
- Specialized workloads, such as design and engineering, legacy apps, and software development testing.

Personal and pooled desktops

By using personal desktop solutions, sometimes called *persistent desktops*, users can always connect to the same specific session host. Users can ordinarily modify their desktop experience to meet personal preferences, and they can save files in the desktop environment. Personal desktop solutions:

- Let users customize their desktop environment, including user-installed applications, and users can save files within the desktop environment.
- Allow assigning dedicated resources to specific users, which can be helpful for some manufacturing or development use cases.

Pooled desktop solutions, also called *non-persistent desktops*, assign users to whichever session host is currently available, depending on the load-balancing algorithm. Because users don't always return to the same session host each time they connect, they have limited ability to customize the desktop environment and don't usually have administrator access.

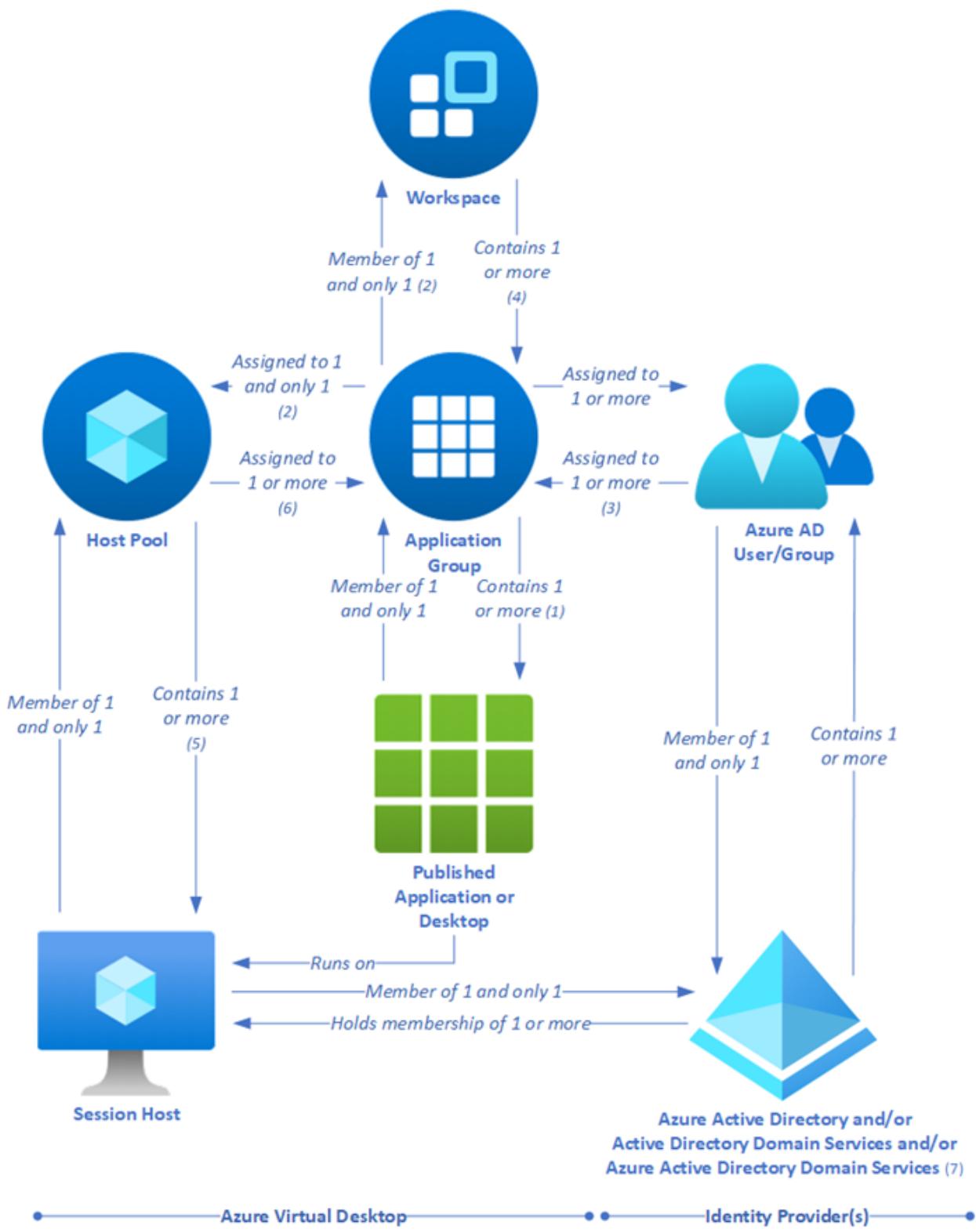
Windows servicing

There are several options for updating Azure Virtual Desktop instances. Deploying an updated image every month guarantees compliance and state.

- [Microsoft Endpoint Configuration Manager \(MECM\)](#) updates server and desktop operating systems.
- [Windows Updates for Business](#) updates desktop operating systems such as Windows 10 multi-session.
- [Azure Update Management](#) updates server operating systems.
- [Azure Log Analytics](#) checks compliance.
- Deploy a new (custom) image to session hosts every month for the latest Windows and applications updates. You can use an image from Azure Marketplace or a [custom Azure-managed image](#).

Relationships between key logical components

The relationships between host pools, workspaces, and other key logical components vary. They're summarized in the following diagram:



The numbers in the following descriptions correspond to those in the preceding diagram.

- (1) An application group that contains a published desktop can only contain MSIX packages mounted to the host pool (the packages will be available in the *Start* menu of the session host), it can't contain any other published resources and is called a desktop application group.
- (2) Application groups assigned to the same host pool must be members of the same workspace.

- (3) A user account can be assigned to an application group either directly or via a Microsoft Entra group. It's possible to assign no users to an application group, but then it can't service any.
- (4) It's possible to have an empty workspace, but it can't service users.
- (5) It's possible to have an empty host pool, but it can't service users.
- (6) It's possible for a host pool not to have any application groups assigned to it but it can't service users.
- (7) Microsoft Entra ID is required for Azure Virtual Desktop. This is because Microsoft Entra user accounts and groups must always be used to assign users to Azure Virtual Desktop application groups. Microsoft Entra ID is also used to authenticate users into the Azure Virtual Desktop service. Azure Virtual Desktop session hosts can also be members of a Microsoft Entra domain, and in this situation the Azure Virtual Desktop-published applications and desktop sessions will also be launched and run (not just assigned) by using Microsoft Entra accounts.
 - (7) Alternatively, Azure Virtual Desktop session hosts can be members of an AD DS domain, and in this situation the Azure Virtual Desktop-published applications and desktop sessions will be launched and run (but not assigned) by using AD DS accounts. To reduce user and administrative overhead, AD DS can be synchronized with Microsoft Entra ID through Microsoft Entra Connect.
 - (7) Finally, Azure Virtual Desktop session hosts can, instead, be members of a Microsoft Entra Domain Services domain, and in this situation the Azure Virtual Desktop-published applications and desktop sessions will be launched and run (but not assigned) by using Microsoft Entra Domain Services accounts. Microsoft Entra ID is automatically synchronized with Microsoft Entra Domain Services, one way, from Microsoft Entra ID to Microsoft Entra Domain Services only.

[] [Expand table](#)

Resource	Purpose	Logical relationships
Published desktop	A Windows desktop environment that runs on Azure Virtual Desktop session hosts and is delivered to users over the network	Member of one and only one application group (1)
Published application	A Windows application that runs on Azure Virtual	Member of one and only one application group

Resource	Purpose	Logical relationships
Application group	A logical grouping of published applications or a published desktop	<ul style="list-style-type: none"> - Contains a published desktop (1) or one or more published applications - Assigned to one and only one host pool (2) - Member of one and only one workspace (2) - One or more Microsoft Entra user accounts or groups are assigned to it (3)
Microsoft Entra user account/group	Identifies the users who are permitted to launch published desktops or applications	<ul style="list-style-type: none"> - Member of one and only one Microsoft Entra ID - Assigned to one or more application groups (3)
Microsoft Entra ID (7)	Identity provider	<ul style="list-style-type: none"> - Contains one or more user accounts or groups, which must be used to assign users to application groups, and can also be used to log in to the session hosts - Can hold the memberships of the session hosts - Can be synchronized with AD DS or Microsoft Entra Domain Services
AD DS (7)	Identity and directory services provider	<ul style="list-style-type: none"> - Contains one or more user accounts or groups, which can be used to log in to the session hosts - Can hold the memberships of the session hosts - Can be synchronized with Microsoft Entra ID
Microsoft Entra Domain Services (7)	Platform as a service (PaaS)-based identity and directory services provider	<ul style="list-style-type: none"> - Contains one or more user accounts or groups, which can be used to log in to the session hosts - Can hold the memberships of the session hosts

Resource	Purpose	Logical relationships
		- Synchronized with Microsoft Entra ID
Workspace	A logical grouping of application groups	Contains one or more application groups (4)
Host pool	A group of identical session hosts that serve a common purpose	- Contains one or more session hosts (5) - One or more application groups are assigned to it (6)
Session host	A virtual machine that hosts published desktops or applications	Member of one and only one host pool

Considerations

These considerations implement the pillars of the Azure Well-Architected Framework, which is a set of guiding tenets that can be used to improve the quality of a workload. For more information, see [Microsoft Azure Well-Architected Framework](#).

The numbers in the following sections are approximate. They're based on a variety of large customer deployments and are subject to change over time.

Also, note that:

- You can't create more than 500 application groups per single Microsoft Entra tenant*.
- We recommend that you do *not* publish more than 50 applications per application group.

Azure Virtual Desktop limitations

Azure Virtual Desktop, much like Azure, has certain service limitations that you need to be aware of. To avoid having to make changes in the scaling phase, it's a good idea to address some of these limitations during the design phase.

Expand table

Azure Virtual Desktop object	Per Parent container object	Service limit
Workspace	Microsoft Entra tenant	1300
HostPool	Workspace	400
Application group	Microsoft Entra tenant	500*
RemoteApp	Application group	500
Role assignment	Any Azure Virtual Desktop object	200
Session host	HostPool	10,000

*If you require more than 500 application groups, submit a support ticket via the Azure portal.

- We recommend that you deploy no more than 5,000 VMs per Azure subscription per region. This recommendation applies to both personal and pooled host pools, based on Windows Enterprise single and multi-session. Most customers use Windows Enterprise multi-session, which allows multiple users to log in to each VM. You can increase the resources of individual session-host VMs to accommodate more user sessions.
- For automated session-host scaling tools, the limits are around 2,500 VMs per Azure subscription per region, because VM status interaction consumes more resources.
- To manage enterprise environments with more than 5,000 VMs per Azure subscription in the same region, you can create multiple Azure subscriptions in a hub-spoke architecture and connect them via virtual network peering (using one subscription per spoke). You could also deploy VMs in a different region in the same subscription to increase the number of VMs.
- Azure Resource Manager (ARM) subscription API throttling limits don't allow more than 600 Azure VM reboots per hour via the Azure portal. You can reboot all your machines at once via the operating system, which doesn't consume any Azure Resource Manager subscription API calls. For more information about counting and troubleshooting throttling limits based on your Azure subscription, see [Troubleshoot API throttling errors](#).
- You can currently deploy up to 132 VMs in a single ARM template deployment in the Azure Virtual Desktop portal. To create more than 132 VMs, run the ARM

template deployment in the Azure Virtual Desktop portal multiple times.

- Azure VM session-host name prefixes can't exceed 11 characters, due to auto-assigning of instance names and the NetBIOS limit of 15 characters per computer account.
- By default, you can deploy up to 800 instances of most resource types in a resource group. Azure Compute doesn't have this limit.

For more information about Azure subscription limitations, see [Azure subscription and service limits, quotas, and constraints](#).

VM sizing

[Virtual machine sizing guidelines](#) lists the maximum suggested number of users per virtual central processing unit (vCPU) and minimum VM configurations for different workloads. This data helps estimate the VMs you need in your host pool.

Use simulation tools to test deployments with both stress tests and real-life usage simulations. Make sure that the system is responsive and resilient enough to meet user needs, and remember to vary the load sizes when testing.

Cost optimization

Cost optimization is about looking at ways to reduce unnecessary expenses and improve operational efficiencies. For more information, see [Overview of the cost optimization pillar](#).

You can architect your Azure Virtual Desktop solution to realize cost savings. Here are five different options to help manage costs for enterprises:

- **Windows 10 multi-session:** By delivering a multi-session desktop experience for users with identical compute requirements, you can let more users log in to a single VM at once, an approach that can result in considerable cost savings.
- **Azure Hybrid Benefit:** If you have Software Assurance, you can use [Azure Hybrid Benefit for Windows Server](#) to save on the cost of your Azure infrastructure.
- **Azure Reserved VM Instances:** You can prepay for your VM usage and save money. Combine [Azure Reserved VM Instances](#) with Azure Hybrid Benefit for up to 80 percent savings over list prices.
- **Session-host load-balancing:** When you're setting up session hosts, *breadth-first* mode, which spreads users randomly across the session hosts, is the standard default mode. Alternatively, you can use *depth-first* mode to fill up a session-host server with the maximum number of users before it moves on to the next session host. You can adjust this setting for maximum cost benefits.

Deploy this scenario

Use the [ARM templates](#) to automate the deployment of your Azure Virtual Desktop environment. These ARM templates support only Azure Resource Manager's Azure Virtual Desktop objects. These ARM templates don't support Azure Virtual Desktop (classic).

Contributors

This article is maintained by Microsoft. It was originally written by the following contributors.

Principal author:

- [Tom Hickling](#) | Senior Product Manager, Azure Virtual Desktop Engineering

Other contributor:

- [Nelson Del Villar](#) | Cloud Solution Architect, Azure Core Infrastructure

Next steps

- [Azure Virtual Desktop partner integrations](#) lists approved Azure Virtual Desktop partner providers and independent software vendors.
- Use the [Virtual Desktop Optimization Tool](#) to help optimize performance in a Windows 10 Enterprise VDI (virtual desktop infrastructure) environment.
- See [Deploy Microsoft Entra joined virtual machines in Azure Virtual Desktop](#).
- Learn more about [Active Directory Domain Services](#).
- [What is Microsoft Entra Connect?](#)

Related resources

- For more information about multiple Active Directory forests architecture, see [Multiple Active Directory forests architecture in Azure Virtual Desktop](#).

Computer forensics chain of custody in Azure

Azure Automation

Azure Disk Encryption

Azure Key Vault

Azure Storage Accounts

This article describes an infrastructure and workflow process that helps teams ensure that the digital evidence they provide in response to legal requests demonstrates a valid *chain of custody* (CoC). This discussion helps ensure a valid CoC throughout the evidence acquisition, preservation, and access processes.

ⓘ Note

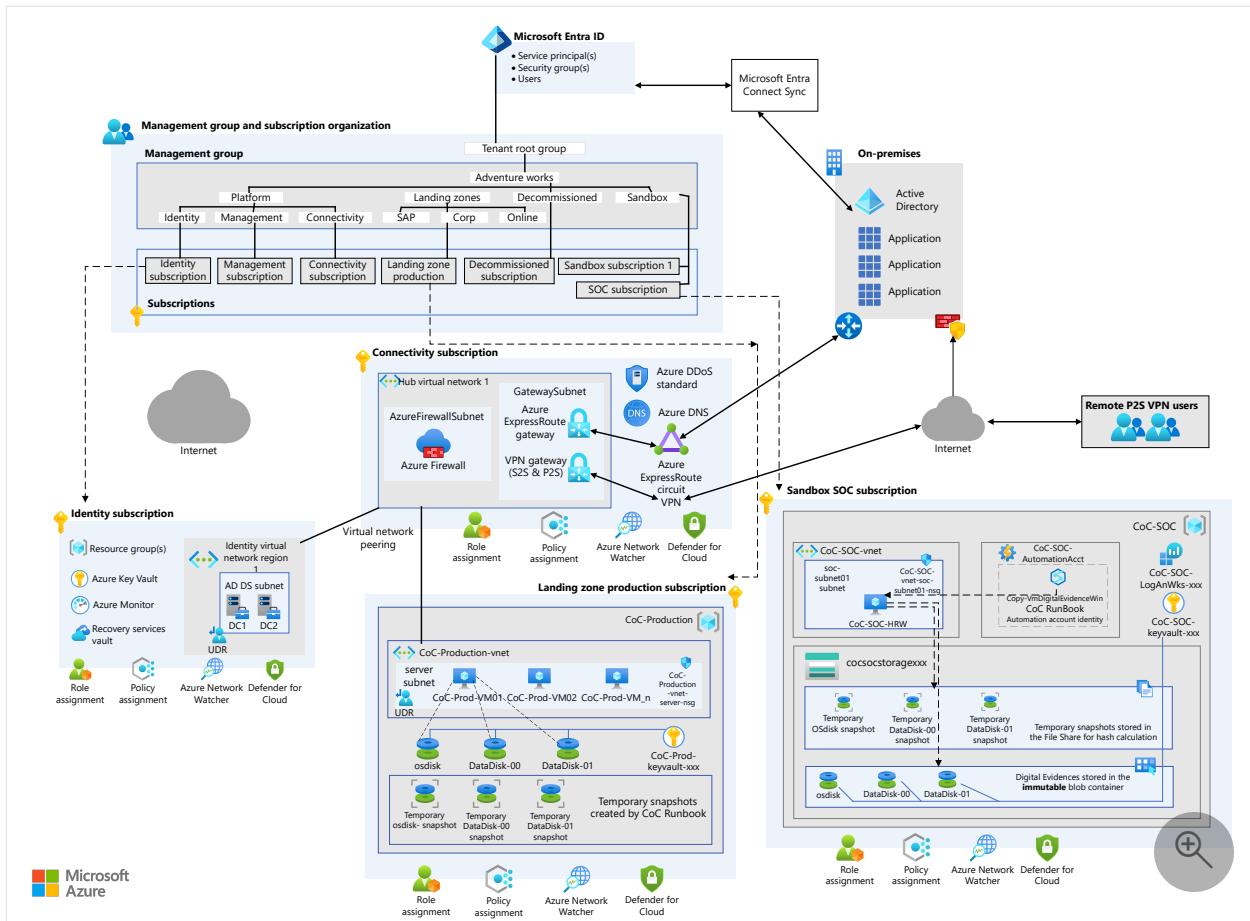
This article is based on the theoretical and practical knowledge of the authors.

Before you use it for legal purposes, you should validate its applicability with your legal department.

Architecture

The architecture design follows the [Azure landing zone](#) principles that are described in the [Cloud Adoption Framework for Azure](#).

This scenario uses a hub-and-spoke network topology as shown in the following diagram:



Download a [Visio file](#) of this architecture.

Workflow

In the architecture, the production virtual machines (VMs) are part of a spoke [Azure virtual network](#). Their disks are encrypted with Azure Disk Encryption. For more information, see [Overview of managed disk encryption options](#). In the production subscription, [Azure Key Vault](#) stores the VMs' BitLocker encryption keys (BEKs).

ⓘ Note

The scenario works for production VMs with unencrypted disks.

The system and organization controls (SOC) team uses a discrete Azure [SOC](#) subscription. The team has exclusive access to that subscription, which contains the resources that must be kept protected, inviolable, and monitored. The [Azure Storage](#) account in the SOC subscription hosts copies of disk snapshots in [immutable blob storage](#), and a dedicated [key vault](#) keeps the snapshots' hash values and copies of the VMs' BEKs.

In response to a request to capture a VM's digital evidence, a SOC team member signs in to the Azure SOC subscription and uses a [hybrid runbook worker](#) VM in [Automation](#)

to implement the Copy-VmDigitalEvidence runbook. The [Automation hybrid runbook worker](#) provides control of all mechanisms involved in the capture.

The Copy-VmDigitalEvidence runbook implements these macro steps:

1. Sign in to Azure by using the [System-assigned managed identity for an Automation account](#) to access the target VM's resources and the other Azure services required by the solution.
2. Create disk snapshots for the VM's operating system (OS) and data disks.
3. Copy the snapshots to the SOC subscription's immutable blob storage, and in a temporary file share.
4. Calculate hash values of the snapshots by using the copy on the file share.
5. Copy the obtained hash values and the VM's BEK in the SOC key vault.
6. Clean up all the copies of the snapshots except the one in immutable blob storage.

ⓘ Note

The production VMs' encrypted disks can also use *key encryption keys* (KEKs). The Copy-VmDigitalEvidence runbook provided in the [deploy scenario](#) doesn't cover this scenario.

Components

- [Azure Automation](#) automates frequent, time-consuming, and error-prone cloud management tasks.
- [Storage](#) is a cloud storage solution that includes object, file, disk, queue, and table storage.
- [Azure Blob Storage](#) provides optimized cloud object storage that manages massive amounts of unstructured data.
- [Azure Files](#) shares can be mounted concurrently by cloud or on-premises deployments of Windows, Linux, and macOS. Azure Files shares can also be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.
- [Azure Monitor](#) supports your operations at scale by helping you maximize the performance and availability of your resources and proactively identify problems.
- [Key Vault](#) helps you safeguard cryptographic keys and other secrets used by cloud apps and services.
- [Microsoft Entra ID](#) is a cloud-based identity service that helps you control access to Azure and other cloud apps.

Automation

The SOC team uses an [Automation](#) account to create and maintain the Copy-VmDigitalEvidence runbook. The team also uses [Automation](#) to create the hybrid runbook workers that run the runbook.

Hybrid runbook worker

The [hybrid runbook worker](#) VM is part of the Automation account and is used exclusively by the SOC team to implement the Copy-VmDigitalEvidence runbook.

You must place the hybrid runbook worker VM in a subnet that can access the Storage account. Access to the Storage account is configured by adding the hybrid runbook worker VM subnet to the Storage account's firewall allowlist rules.

You must grant access to this VM only to the SOC team members for maintenance activities.

To isolate the virtual network that's used by the VM, don't connect that virtual network to the hub.

The hybrid runbook worker uses the [Automation system-assigned managed identity](#) to access the target VM's resources and the other Azure services required by the solution.

The minimal role-based access control (RBAC) permissions that must be assigned to system-assigned managed identity are classified in two categories:

- Access permissions to the SOC Azure architecture containing the solution core components
- Access permissions to the target architecture containing the target VM resources

Access to the SOC Azure architecture includes the following roles:

- **Storage Account Contributor** on the SOC immutable Storage account
- **Key Vault Secrets Officer** on the SOC key vault for the BEK management

Access to the target architecture includes the following roles:

- **Contributor** on the target VM's resource group, which provides snapshot rights on VM disks
- **Key Vault Secrets Officer** on the target VM's key vault used to store BEK, only if RBAC is used for the key vault
- Access policy to **Get Secret** on the target VM's key vault used to store BEK, only if you use an access policy for Key Vault

(!) Note

To read the BEK, the target VM's key vault must be accessible from the hybrid runbook worker VM. If the key vault has the firewall enabled, ensure that the public IP address of the hybrid runbook worker VM is allowed through the firewall.

Azure Storage account

The [Azure Storage account](#) in the SOC subscription hosts the disk snapshots in a container configured with a *legal hold* policy as Azure immutable blob storage. Immutable blob storage stores business-critical data objects in a *write once, read many* (WORM) state, which makes the data nonerasable and uneditable for a user-specified interval.

Ensure the [secure transfer](#) and [storage firewall](#) properties are both enabled. The firewall grants access only from the SOC virtual network.

The storage account also hosts an [Azure file share](#) used as a temporary repository for calculating the snapshot's hash value.

Azure Key Vault

The SOC subscription has its own instance of [Key Vault](#), which hosts a copy of the BEK that Azure Disk Encryption uses to protect the target VM. The primary copy is kept in the key vault that is used by the target VM, so that the target VM can continue normal operation.

The SOC key vault also contains the hash values of disk snapshots calculated by the hybrid runbook worker during the capture operations.

Ensure the [firewall](#) is enabled on the key vault. It's configured to grant access only from the SOC virtual network.

Log Analytics

A [Log Analytics workspace](#) stores activity logs used to audit all relevant events on the SOC subscription. Log Analytics is a feature of [Monitor](#).

Scenario details

Digital forensics is a science that addresses the recovery and investigation of digital data to support criminal investigations or civil proceedings. Computer forensics is a branch of digital forensics that captures and analyzes data from computers, VMs, and digital storage media.

Companies must guarantee that the digital evidence they provide in response to legal requests demonstrates a valid CoC throughout the evidence acquisition, preservation, and access process.

Potential use cases

- A company's Security Operation Center team can implement this technical solution to support a valid CoC for digital evidence.
- Investigators can attach disk copies that are obtained with this technique on a computer dedicated to forensic analysis. They can attach the disk copies without powering on or accessing the original source VM.

CoC regulatory compliance

If it's necessary to submit the proposed solution to a regulatory compliance validation process, consider the topics in [considerations](#) during the CoC solution validation process.

ⓘ Note

You should involve your legal department in the process of validation.

Considerations

The principles that validate this solution as a Chain of Custody (CoC) are being presented in this section.

To ensure a valid CoC, digital evidence storage must demonstrate adequate access control, data protection and integrity, monitoring and alerting, and logging and auditing.

Compliance with security standards and regulations

When you validate a CoC solution, one of the requirements to evaluate is the compliance with security standards and regulations.

All the components included in the [architecture](#) are Azure standard services built upon a foundation that supports trust, security, and [compliance](#) ↗.

Azure has a wide range of compliance certifications, including certifications specific for countries or regions, and for the key industries like healthcare, government, finance, and education.

For updated audit reports with information about standards compliance for the services that are adopted in this solution, see [Service Trust Portal](#) ↗.

Cohasset's [Azure Storage: SEC 17a-4\(f\) and CFTC 1.31\(c\)-\(d\) Compliance Assessment](#) ↗ gives details on the following requirements:

- Securities and Exchange Commission (SEC) in 17 CFR § 240.17a-4(f), which regulates exchange members, brokers, or dealers.
- Financial Industry Regulatory Authority (FINRA) Rule 4511(c), which defers to the format and media requirements of SEC Rule 17a-4(f).
- Commodity Futures Trading Commission (CFTC) in regulation 17 CFR § 1.31(c)-(d), which regulates commodity futures trading.

It's Cohasset's opinion that Storage, with the Immutable Storage for Azure blobs feature and policy lock option, retains *time-based* blobs (records) in a nonerasable and nonrewriteable format and meets relevant storage requirements of SEC Rule 17a-4(f), FINRA Rule 4511(c), and the principles-based requirements of CFTC Rule 1.31(c)-(d).

Least privilege

When the roles of the SOC team are assigned, only two individuals within the team should have rights to modify the RBAC configuration of the subscription and its data. Grant other individuals only bare minimum access rights to data subsets they need to perform their work. Configure and enforce access through [Azure RBAC](#).

Least access

Only the [virtual network](#) in the SOC subscription has access to the SOC Storage account and key vault that is used to archive the evidence.

Temporary access to the SOC storage is provided to investigators that require access to evidence. Authorized SOC team members can grant access.

Evidence acquisition

Azure audit logs can show the evidence acquisition by recording the action of taking a VM disk snapshot, with elements like who has taken the snapshots and when.

Evidence integrity

The use of Automation to move evidence to its final archive destination, without human intervention, guarantees that evidence artifacts haven't been altered.

When you apply a legal hold policy to the destination storage, the evidence is frozen in time as soon as it's written. A legal hold shows that the CoC has been maintained entirely in Azure. A legal hold also shows that there wasn't an opportunity to tamper between the time the disk images existed on a live VM and when they were added as evidence in the storage account.

Lastly, you can use the provided solution, as an integrity mechanism, to calculate the hash values of the disk images. The supported hash algorithms are: MD5, SHA256, SKEIN, KECCAK (or SHA3).

Evidence production

Investigators need access to evidence to perform analyses, and this access must be tracked and explicitly authorized.

Provide investigators with a storage [shared access signatures \(SAS\) URI](#) key for accessing evidence. You can use an SAS URI to produce relevant log information when the SAS is generated. You can also get a copy of the evidence every time the SAS is used.

You must explicitly place the IP addresses of investigators requiring access on an allowlist in the Storage firewall.

For example, if a legal team needs to transfer a preserved virtual hard drive (VHD), one of the two SOC team custodians generates a read-only SAS URI key that expires after eight hours. The SAS limits the access to the IP addresses of the investigators to a specific time frame.

Finally, investigators need the BEKs archived in the SOC key vault to access the encrypted disk copies. An SOC team member must extract the BEKs and provide them via secure channels to the investigators.

Regional store

For compliance, some standards or regulations require evidence and the support infrastructure to be maintained in the same Azure region.

All the solution components, including the Storage account used to archive evidence, are hosted in the same Azure region as the systems being investigated.

Operational excellence

Operational excellence covers the operations processes that deploy an application and keep it running in production. For more information, see [Overview of the operational excellence pillar](#).

Monitoring and alerting

Azure provides services to all customers to monitor and alert on anomalies involving their subscriptions and resources. These services include:

- [Microsoft Sentinel](#).
- [Microsoft Defender for Cloud](#).
- [Azure Storage Advanced Threat Protection \(ATP\)](#).

 **Note**

The configuration of these services isn't described in this article.

Deploy this scenario

Follow the [CoC LAB Deployment](#) instructions to build and deploy this scenario in a laboratory environment.

The laboratory environment represents a simplified version of the architecture that is described in the article deploying two resource groups within the same subscription. The first resource group simulates the production environment, housing digital evidence, while the second resource group holds the SOC environment.

Use the following button to deploy only the SOC resource group in a production environment.



[Deploy to Azure](#)

ⓘ Note

If you deploy the solution in a production environment, make sure that the system-assigned managed identity of the automation account has following permissions:

- Contributor: in the production resource group of the VM to be processed (needed to create the snapshots)
- Key Vault Secrets User: in the production key vault holding the BEK keys (needed to read the BEK keys)

Additionally, if the key vault has the firewall enabled, ensure that the public IP address of the hybrid runbook worker VM is allowed through the firewall.

Extended configuration

You can deploy a hybrid runbook worker on-premises or in different cloud environments.

In this scenario, you can customize the `Copy-VmDigitalEvidence` runbook to enable the capture of evidence in different target environments and archive them in storage.

ⓘ Note

The `Copy-VmDigitalEvidence` runbook provided in the [Deploy this scenario](#) section has been developed and tested only in Azure. To extend the solution to other platforms, you must customize the runbook to work with those platforms.

Contributors

This article is maintained by Microsoft. It was originally written by the following contributors.

Principal author:

- [Fabio Masciotra](#) | Principal Consultant
- [Simone Savi](#) | Senior Consultant

To see non-public LinkedIn profiles, sign in to LinkedIn.

Next steps

For more information about Azure data-protection features, see:

- [Azure Storage encryption for data at rest](#)
- [Overview of managed disk encryption options](#)
- [Store business-critical blob data with immutable storage](#)

For more information about Azure logging and auditing features, see:

- [Azure security logging and auditing](#)
- [Azure Storage analytics logging](#)
- [Azure resource logs](#)

For more information about Microsoft Azure Compliance, see:

- [Azure compliance ↗](#)
- [Microsoft Azure Compliance Offerings ↗](#)

Related resources

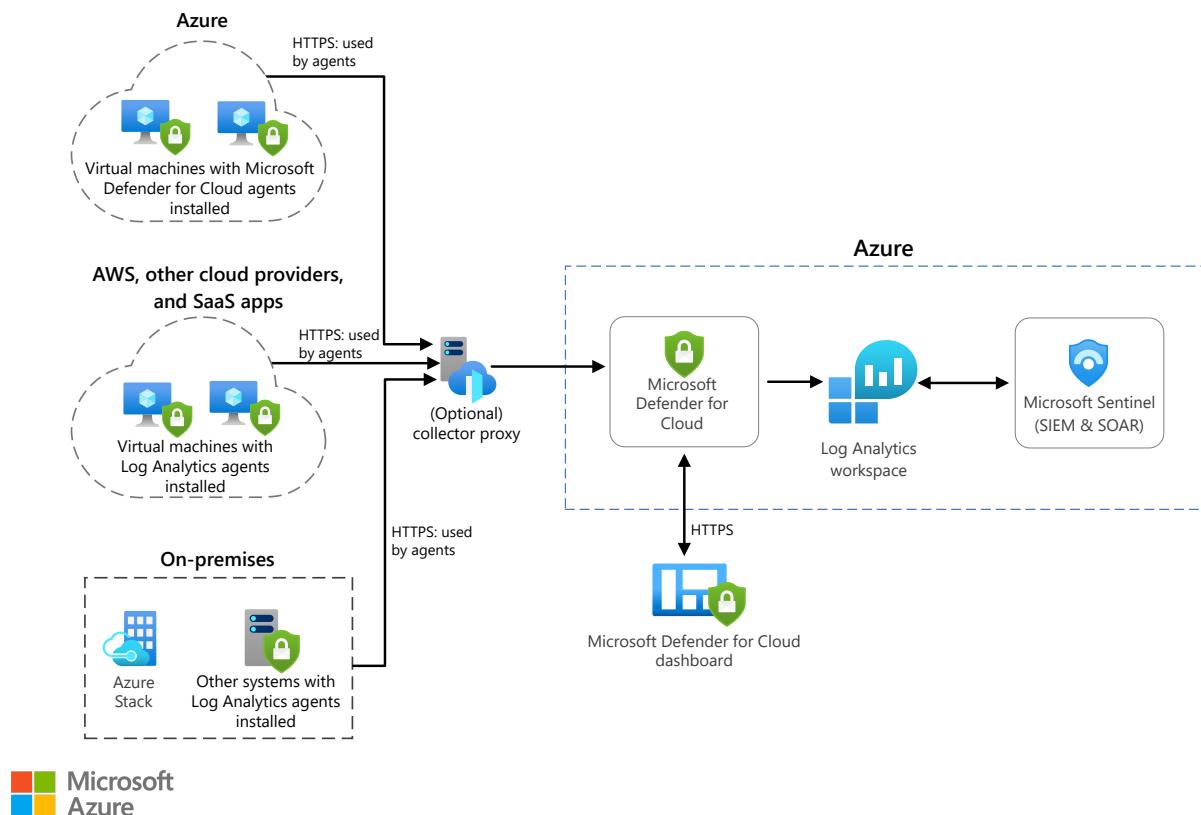
- [Security architecture design](#)
- [Microsoft Entra IDaaS in security operations](#)
- [Security considerations for highly sensitive IaaS apps in Azure](#)

Monitor hybrid security using Microsoft Defender for Cloud and Microsoft Sentinel

Azure Log Analytics Azure Monitor Microsoft Defender for Cloud Microsoft Sentinel Azure Stack

This reference architecture illustrates how to use Microsoft Defender for Cloud and Microsoft Sentinel to monitor the security configuration and telemetry of on-premises, Azure, and Azure Stack workloads.

Architecture



Download a [Visio file](#) of this architecture.

Workflow

- **Microsoft Defender for Cloud.** This is an advanced, unified security-management platform that Microsoft offers to all Azure subscribers. Defender for Cloud is segmented as a cloud security posture management (CSPM) and cloud workload

protection platform (CWPP). CWPP is defined by workload-centric security protection solutions, which are typically agent-based. Microsoft Defender for Cloud provides threat protection for Azure workloads, both on-premises and in other clouds, including Windows and Linux virtual machines (VMs), containers, databases, and Internet of Things (IoT). When activated, the Log Analytics agent deploys automatically into Azure Virtual Machines. For on-premises Windows and Linux servers and VMs, you can manually deploy the agent, use your organization's deployment tool, such as Microsoft Endpoint Protection Manager, or utilize scripted deployment methods. Defender for Cloud begins assessing the security state of all your VMs, networks, applications, and data.

- **Microsoft Sentinel.** Is a cloud-native Security Information and Event Management (SIEM) and security orchestration automated response (SOAR) solution that uses advanced AI and security analytics to help you detect, hunt, prevent, and respond to threats across your enterprise.
- **Azure Stack.** Is a portfolio of products that extend Azure services and capabilities to your environment of choice, including the datacenter, edge locations, and remote offices. Azure Stack implementations typically utilize racks of four to sixteen servers that are built by trusted hardware partners and delivered to your datacenter.
- **Azure Monitor.** Collects monitoring telemetry from a variety of on-premises and Azure sources. Management tools, such as those in Microsoft Defender for Cloud and Azure Automation, also push log data to Azure Monitor.
- **Log Analytics workspace.** Azure Monitor stores log data in a Log Analytics workspace, which is a container that includes data and configuration information.
- **Log Analytics agent.** The Log Analytics agent collects monitoring data from the guest operating system and VM workloads in Azure, from other cloud providers, and from on-premises. The Log Analytics Agent supports Proxy configuration and, typically in this scenario, a Microsoft Operations Management Suite (OMS) Gateway acts as proxy.
- **On-premises network.** This is the firewall configured to support HTTPS egress from defined systems.
- **On-premises Windows and Linux systems.** Systems with the Log Analytics Agent installed.
- **Azure Windows and Linux VMs.** Systems on which the Microsoft Defender for Cloud monitoring agent is installed.

Components

- [Microsoft Defender for Cloud ↗](#)
- [Microsoft Sentinel ↗](#)

- [Azure Stack](#)
- [Azure Monitor](#)

Scenario details

Potential use cases

Typical uses for this architecture include:

- Best practices for integrating on-premises security and telemetry monitoring with Azure-based workloads
- Integrating Microsoft Defender for Cloud with Azure Stack
- Integrating Microsoft Defender for Cloud with Microsoft Sentinel

Recommendations

The following recommendations apply for most scenarios. Follow these recommendations unless you have a specific requirement that overrides them.

Microsoft Defender for Cloud upgrade

This reference architecture uses **Microsoft Defender for Cloud** to monitor on-premises systems, Azure VMs, Azure Monitor resources, and even VMs hosted by other cloud providers. Details about Microsoft Defender for Cloud pricing can be found [here](#).

Customized Log Analytics Workspace

Microsoft Sentinel needs access to a Log Analytics workspace. In this scenario, you can't use the default Defender for Cloud Log Analytics workspace with Microsoft Sentinel. Instead, you create a customized workspace. Data retention for a customized workspace is based on the workspace pricing tier, and you can find pricing models for Monitor Logs [here](#).

Note

Microsoft Sentinel can run on workspaces in any general availability (GA) region of Log Analytics except the China and Germany (Sovereign) regions. Data that Microsoft Sentinel generates, such as incidents, bookmarks, and alert rules, which may contain some customer data sourced from these workspaces, is saved either in

Europe (for Europe-based workspaces), in Australia (for Australia-based workspaces), or in the East US (for workspaces located in any other region).

Considerations

These considerations implement the pillars of the Azure Well-Architected Framework, which is a set of guiding tenets that can be used to improve the quality of a workload. For more information, see [Microsoft Azure Well-Architected Framework](#).

Security

Security provides assurances against deliberate attacks and the abuse of your valuable data and systems. For more information, see [Overview of the security pillar](#).

A **security policy** defines the set of controls that are recommended for resources within a specified subscription. In Microsoft Defender for Cloud, you define policies for your Azure subscriptions according to the security requirements of your company and the type of applications or data sensitivity for each subscription.

The security policies that you enable in Microsoft Defender for Cloud drive security recommendations and monitoring. To learn more about security policies, refer to [Strengthen your security policy with Microsoft Defender for Cloud](#). You can assign security policies in Microsoft Defender for Cloud only at the management or subscription group levels.

Note

Part one of the reference architecture details how to enable Microsoft Defender for Cloud to monitor Azure resources, on-premises systems, and Azure Stack systems.

Cost optimization

Cost optimization is about looking at ways to reduce unnecessary expenses and improve operational efficiencies. For more information, see [Overview of the cost optimization pillar](#).

As previously described, costs beyond your Azure subscription can include:

1. Microsoft Defender for Cloud costs. For more information, refer to [Defender for Cloud pricing](#).

2. Azure Monitor workspace offers granularity of billing. For more information, refer to [Manage Usage and Costs with Azure Monitor Logs](#).
3. Microsoft Sentinel is a paid service. For more information, refer to [Microsoft Sentinel pricing](#).

Operational excellence

Operational excellence covers the operations processes that deploy an application and keep it running in production. For more information, see [Overview of the operational excellence pillar](#).

Microsoft Defender for Cloud roles

Defender for Cloud assesses the configuration of your resources to identify security issues and vulnerabilities, and displays information related to a resource when you are assigned the role of owner, contributor, or reader for the subscription or resource group to which a resource belongs.

In addition to these roles, there are two specific Defender for Cloud roles:

- **Security Reader.** A user that belongs to this role has read only rights to Defender for Cloud. The user can observe recommendations, alerts, a security policy, and security states, but can't make changes.
- **Security Admin.** A user that belongs to this role has the same rights as the Security Reader, and also can update security policies, and dismiss alerts and recommendations. Typically, these are users that manage the workload.
- The security roles, **Security Reader** and **Security Admin**, have access only in Defender for Cloud. The security roles don't have access to other Azure service areas, such as storage, web, mobile, or IoT.

Microsoft Sentinel subscription

- To enable Microsoft Sentinel, you need contributor permissions to the subscription in which the Microsoft Sentinel workspace resides.
- To use Microsoft Sentinel, you need contributor or reader permissions on the resource group to which the workspace belongs.
- Microsoft Sentinel is a paid service. For more information, refer to [Microsoft Sentinel pricing](#).

Performance efficiency

Performance efficiency is the ability of your workload to scale in an efficient manner to meet the demands that users place on it. For more information, see [Performance efficiency pillar overview](#).

The Log Analytics Agent for Windows and Linux is designed to have very minimal impact on the performance of VMs or physical systems.

Microsoft Defender for Cloud operational process won't interfere with your normal operational procedures. Instead, it passively monitors your deployments and provides recommendations based on the security policies you enable.

Deploy this scenario

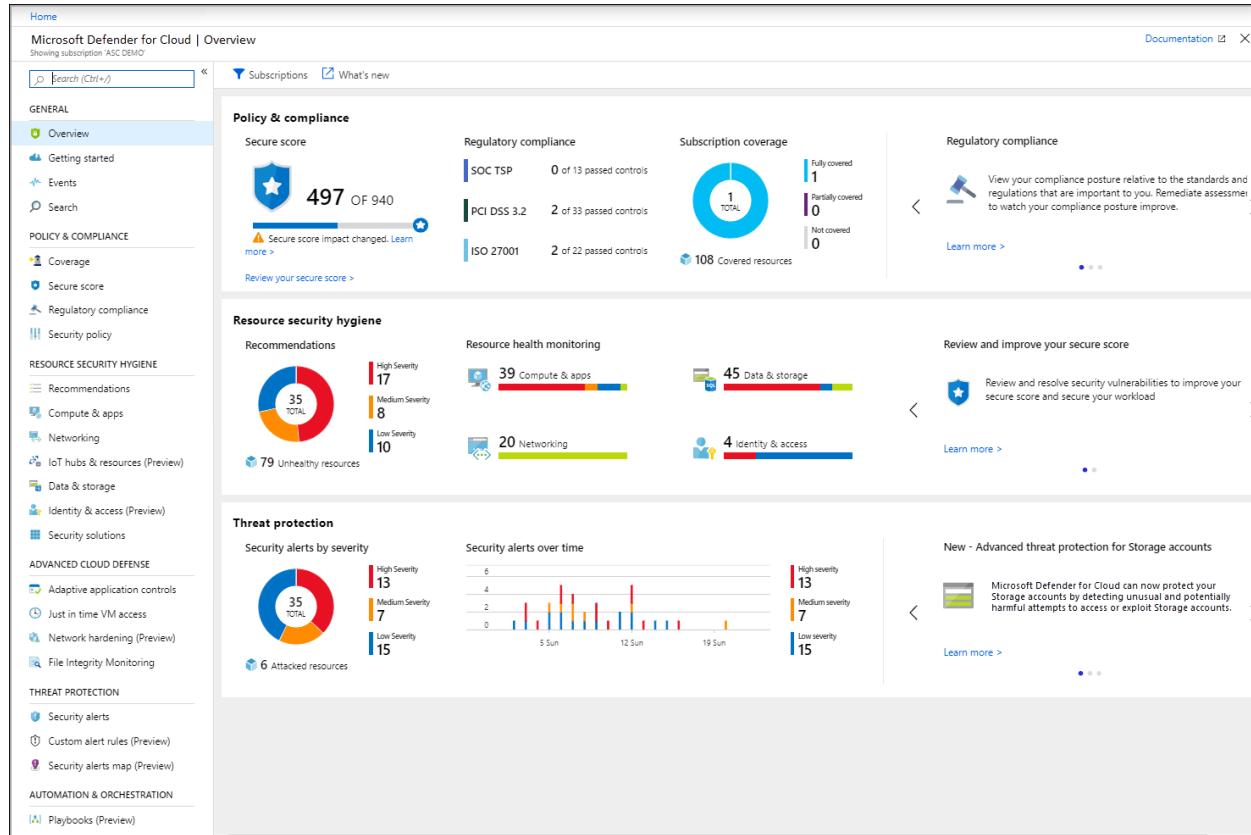
Create a Log Analytics workspace in the Azure portal

1. Sign into the Azure portal as a user with Security Admin privileges.
2. In the Azure portal, select **All services**. In the list of resources, enter **Log Analytics**. As you begin entering, the list filters based on your input. Select **Log Analytics workspaces**.
3. Select **Add** on the Log Analytics page.
4. Provide a name for the new Log Analytics workspace, such as **Defender for Cloud-SentinelWorkspace**. This name must be globally unique across all Azure Monitor subscriptions.
5. Select a subscription by selecting from the drop-down list if the default selection is not appropriate.
6. For **Resource Group**, choose to use an existing resource group or create a new one.
7. For **Location**, select an available geolocation.
8. Select **OK** to complete the configuration.

NAME	TYPE	LOCATION	...
myAKSCluster	Kubernetes service	East US	...
ASC-SentinelWorkspace	Log Analytics	East US	...

Enable Defender for Cloud

While you're still signed into the Azure portal as a user with Security Admin privileges, select **Defender for Cloud** in the panel. **Defender for Cloud - Overview** opens:



The screenshot shows the Microsoft Defender for Cloud - Overview page. The left sidebar contains a navigation menu with sections like Home, Overview, Getting started, Events, Search, Policy & Compliance, Resource Security Hygiene, Advanced Cloud Defense, Threat Protection, and Automation & Orchestration. The main content area is divided into several sections: **Policy & compliance** (Secure score: 497 of 940, Regulatory compliance: SOC TSP 0/13, PCI DSS 3.2 2/33, ISO 27001 2/22, Subscription coverage: 108 resources), **Resource security hygiene** (Recommendations: 35 total, 79 unhealthy resources, 17 High Severity, 8 Medium Severity, 10 Low Severity), **Threat protection** (Security alerts by severity: 35 total, 6 attacked resources, 13 High severity, 7 Medium severity, 15 Low severity), and **Regulatory compliance** (View your compliance posture relative to the standards and regulations that are important to you. Remediate assessments to watch your compliance posture improve). There are also sections for **Review and improve your secure score** and **New - Advanced threat protection for Storage accounts**.

Defender for Cloud automatically enables the Free tier for any of the Azure subscriptions not previously onboarded by you or another subscription user.

Upgrade Microsoft Defender for Cloud

1. On the Defender for Cloud main menu, select **Getting Started**.
2. Select the **Upgrade Now** button. Defender for Cloud lists your subscriptions and workspaces that are eligible for use.
3. You can select eligible workspaces and subscriptions to start your trial. Select the previously created workspace, **ASC-SentinelWorkspace**, from the drop-down menu.
4. In the Defender for Cloud main menu, select **Start trial**.
5. The **Install Agents** dialog box should display.
6. Select the **Install Agents** button. The **Defender for Cloud - Coverage** blade displays and you should observe your selected subscription.

Security Center - Coverage

Not covered Basic coverage Standard coverage

Looking good! The subscriptions below are fully protected.

3 SUBSCRIPTIONS

NAME	MY ROLE	OWNER	RESOURCES	ID
Contoso IT - demo	Reader	Display Owners	465	<Subscription ID>
QA-RomeCore-OMSTest2-Prod	Contributor	Display Owners	110	<Subscription ID>
ASC DEMO	Contributor	Display Owners	104	<Subscription ID>

You've now enabled automatic provisioning and Defender for Cloud will install the Log Analytics Agent for Windows (**HealthService.exe**) and the **omsagent** for Linux on all supported Azure VMs and any new ones that you create. You can turn off this policy and manually manage it, although we strongly recommend automatic provisioning.

To learn more about the specific Defender for Cloud features available in Windows and Linux, refer to [Feature coverage for machines](#).

Enable Microsoft Defender for Cloud monitoring of on-premises Windows computers

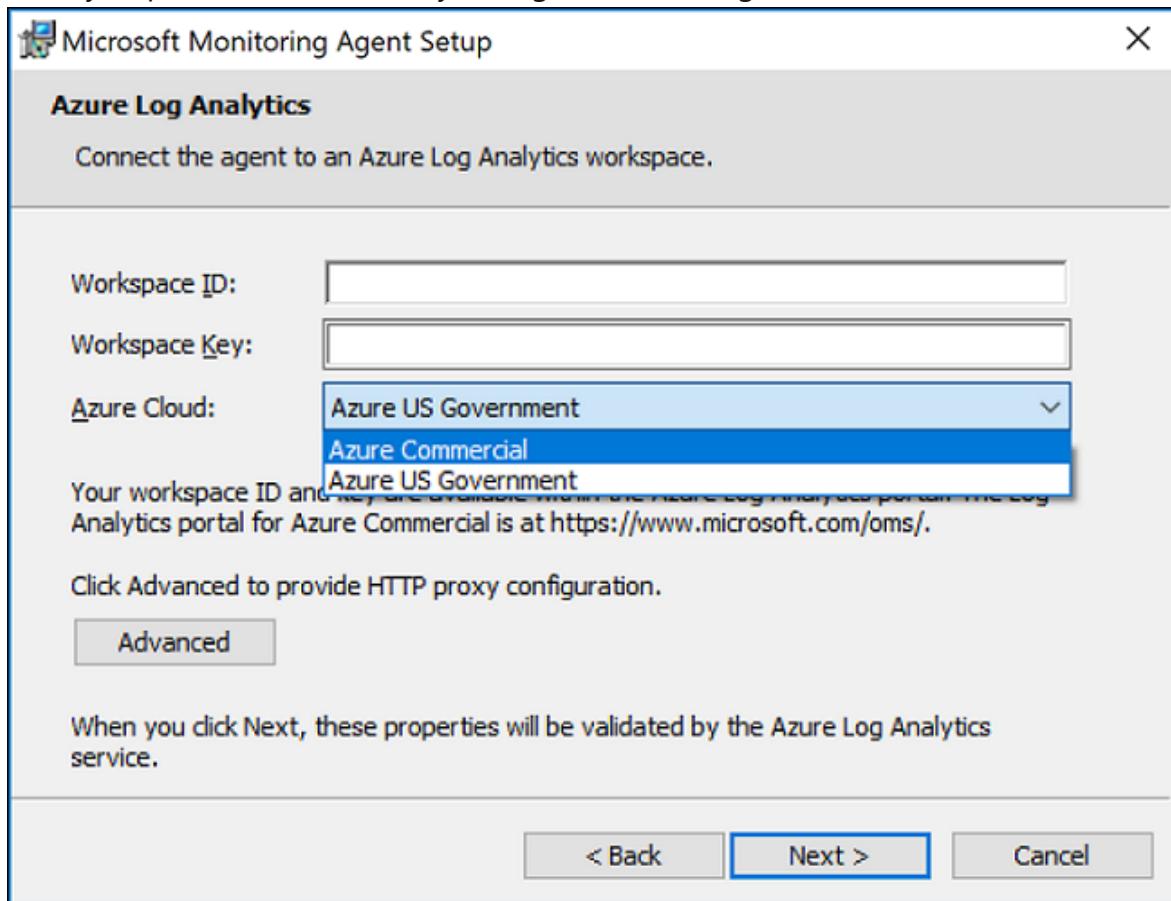
1. In the Azure portal on the **Defender for Cloud - Overview** blade, select the **Get Started** tab.
2. Select **Configure** under **Add new non-Azure computers**. A list of your Log Analytics workspaces displays, and should include the **Defender for Cloud-SentinelWorkspace**.
3. Select this workspace. The **Direct Agent** blade opens with a link for downloading a Windows agent and keys for your workspace identification (ID) to use when you configure the agent.
4. Select the **Download Windows Agent** link applicable to your computer processor type to download the setup file.
5. To the right of **Workspace ID**, select **Copy**, and then paste the ID into Notepad.
6. To the right of **Primary Key**, select **Copy**, and then paste the key into Notepad.

Install the Windows agent

To install the agent on the targeted computers, follow these steps.

1. Copy the file to the target computer and then **Run Setup**.
2. On the **Welcome** page, select **Next**.
3. On the **License Terms** page, read the license and then select **I Agree**.
4. On the **Destination Folder** page, change or keep the default installation folder and then select **Next**.

5. On the **Agent Setup Options** page, choose to connect the agent to Azure Log Analytics and then select **Next**.
6. On the **Azure Log Analytics** page, paste the **Workspace ID** and **Workspace Key (Primary Key)** that you copied into Notepad in the previous procedure.
7. If the computer should report to a Log Analytics workspace in Azure Government cloud, select **Azure US Government** from the **Azure Cloud** drop-down list. If the computer needs to communicate through a proxy server to the Log Analytics service, select **Advanced**, and then provide the proxy server's URL and port number.
8. After you provide the necessary configuration settings, select **Next**.



9. On the **Ready to Install** page, review your choices and then select **Install**.
10. On the **Configuration completed successfully** page, select **Finish**.

When complete, the Log Analytics agent appears in Windows Control Panel, and you can review your configuration and verify that the agent is connected.

For further information about installing and configuring the agent, refer to [Install Log Analytics agent on Windows computers](#).

The Log Analytics Agent service collects event and performance data, executes tasks, and other workflows defined in a management pack. Defender for Cloud extends its cloud workload protection platforms by integrating with **Microsoft Defender for Servers**. Together, they provide comprehensive endpoint detection and response (EDR) capabilities.

For more information about Microsoft Defender for Servers, refer to [Onboard servers to the Microsoft Defender for Servers service](#).

Enable Microsoft Defender for Cloud monitoring of on-premises Linux computers

1. Return to the **Getting Started** tab as previously described.
2. Select **Configure** under **Add new non-Azure computers**. A list of your Log Analytics workspaces displays. The list should include the **Defender for Cloud-SentinelWorkspace** that you created.
3. On the **Direct Agent** blade under **DOWNLOAD AND ONBOARD AGENT FOR LINUX**, select **copy** to copy the **wget** command.
4. Open Notepad and then paste this command. Save this file to a location that you can access from your Linux computer.

Note

On Unix and Linux operating systems, **wget** is a tool for non-interactive file downloading from the web. It supports HTTPS, FTPs, and proxies.

The Linux agent uses the Linux Audit Daemon framework. Defender for Cloud integrates functionalities from this framework within the Log Analytics agent, which enables audit records to be collected, enriched, and aggregated into events by using the Log Analytics Agent for Linux. Defender for Cloud continuously adds new analytics that use Linux signals to detect malicious behaviors on cloud and on-premises Linux machines.

For a list of the Linux alerts, refer to the [Reference table of alerts](#).

Install the Linux agent

To install the agent on the targeted Linux computers, follow these steps:

1. On your Linux computer, open the file that you previously saved. Select and copy the entire content, open a terminal console, and then paste the command.
2. Once the installation finishes, you can validate that the **omsagent** is installed by running the **pgrep** command. The command will return the **omsagent** process identifier (PID). You can find the logs for the agent at:
`/var/opt/microsoft/omsagent/"workspace id"/log/`.

It can take up to 30 minutes for the new Linux computer to display in Defender for Cloud.

Enable Microsoft Defender for Cloud monitoring of Azure Stack VMs

After you onboard your Azure subscription, you can enable Defender for Cloud to protect your VMs running on Azure Stack by adding the **Azure Monitor, Update and Configuration Management** VM extension from the Azure Stack marketplace. To do this:

1. Return to the **Getting Started** tab as previously described.
2. Select **Configure** under **Add new non-Azure computers**. A list of your Log Analytics workspaces displays, and it should include the **Defender for Cloud-SentinelWorkspace** that you created.
3. On the **Direct Agent** blade there is a link for downloading the agent and keys for your workspace ID to use during agent configuration. You don't need to download the agent manually. It'll be installed as a VM extension in the following steps.
4. To the right of **Workspace ID**, select **Copy**, and then paste the ID into Notepad.
5. To the right of **Primary Key**, select **Copy**, and then paste the key into Notepad.

Enable Defender for Cloud monitoring of Azure Stack VMs

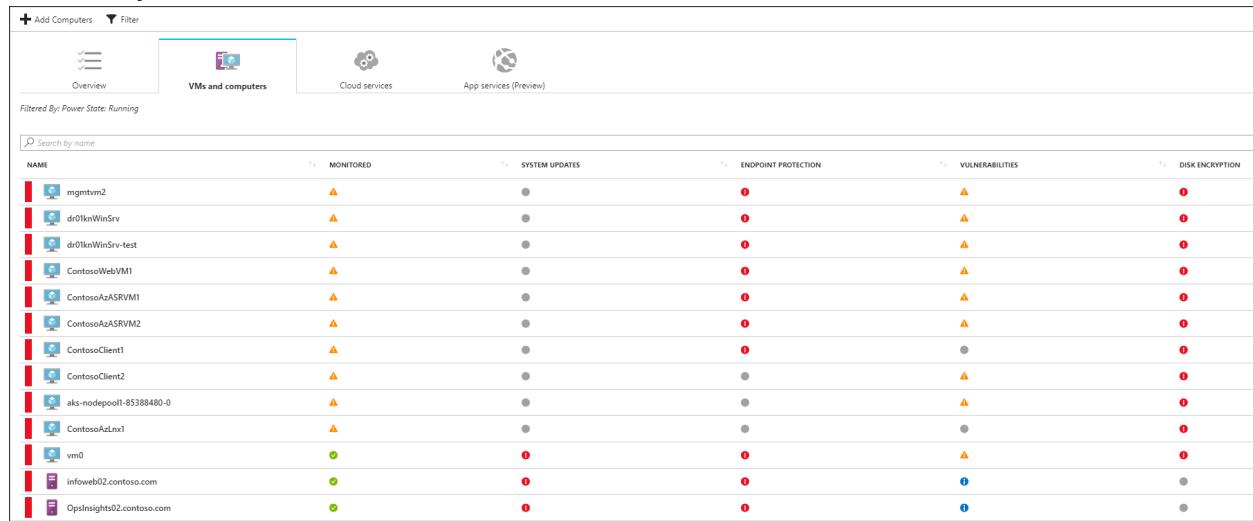
Microsoft Defender for Cloud uses the **Azure Monitor, Update and Configuration Management** VM extension bundled with Azure Stack. To enable the **Azure Monitor, Update and Configuration Management** extension, follow these steps:

1. In a new browser tab, sign into your **Azure Stack** portal.
2. Refer to the **Virtual machines** page, and then select the virtual machine that you want to protect with Defender for Cloud.
3. Select **Extensions**. The list of VM extensions installed on this VM displays.
4. Select the **Add** tab. The **New Resource** menu blade opens and displays the list of available VM extensions.
5. Select the **Azure Monitor, Update and Configuration Management** extension and then select **Create**. The **Install extension** configuration blade opens.
6. On the **Install extension** configuration blade, paste the **Workspace ID** and **Workspace Key (Primary Key)** that you copied into Notepad in the previous procedure.
7. When you finish providing the necessary configuration settings, select **OK**.
8. Once the extension installation completes, its status will display as **Provisioning Succeeded**. It might take up to one hour for the VM to appear in the Defender for Cloud portal.

For more information about installing and configuring the agent for Windows, refer to [Install the agent using setup wizard](#).

For troubleshooting issues for the Linux agent, refer to [How to troubleshoot issues with the Log Analytics agent for Linux](#).

Now you can monitor your Azure VMs and non-Azure computers in one place. **Azure Compute** provides you with an overview of all VMs and computers along with recommendations. Each column represents one set of recommendations, and the color represents the VMs or computers and the current security state for that recommendation. Defender for Cloud also provides any detections for these computers in security alerts.



NAME	MONITORED	SYSTEM UPDATES	ENDPOINT PROTECTION	VULNERABILITIES	DISK ENCRYPTION
mngtvm2	▲	●	●	▲	●
dr01knWinSrv	▲	●	●	▲	●
dr01knWinSrv-test	▲	●	●	▲	●
ContosoWebVM1	▲	●	●	▲	●
ContosoAzASRVM1	▲	●	●	▲	●
ContosoAzASRVM2	▲	●	●	▲	●
ContosoClient1	▲	●	●	●	●
ContosoClient2	▲	●	●	▲	●
aks-nodepool1-85388480-0	▲	●	●	▲	●
ContosoAzLn1	▲	●	●	●	●
vm0	●	●	●	▲	●
infoweb02.contoso.com	●	●	●	●	●
OpsInsights02.contoso.com	●	●	●	●	●

There are two types of icons represented on the **Compute** blade:



Note

Part two of the reference architecture will connect alerts from Microsoft Defender for Cloud and stream them into Microsoft Sentinel.

The role of Microsoft Sentinel is to ingest data from different data sources and perform data correlation across these data sources. Microsoft Sentinel leverages machine learning and AI to make threat hunting, alert detection, and threat responses smarter.

To onboard Microsoft Sentinel, you need to enable it, and then connect your data sources. Microsoft Sentinel comes with a number of connectors for Microsoft solutions, which are available out of the box and provide real-time integration, including Microsoft

Defender for Cloud, Microsoft Threat Protection solutions, Microsoft 365 sources (including Office 365), Microsoft Entra ID, Microsoft Defender for Servers, Microsoft Defender for Cloud Apps, and more. Additionally, there are built-in connectors to the broader security ecosystem for non-Microsoft solutions. You can also use Common Event Format, syslog, or the Representational State Transfer API to connect your data sources with Microsoft Sentinel.

Requirements for integrating Microsoft Sentinel with Microsoft Defender for Cloud

1. A Microsoft Azure Subscription
2. A Log Analytics workspace that isn't the default workspace created when you enable Microsoft Defender for Cloud.
3. Microsoft Defender for Cloud.

All three requirements should be in place if you worked through the previous section.

Global prerequisites

- To enable Microsoft Sentinel, you need contributor permissions to the subscription in which the Microsoft Sentinel workspace resides.
- To use Microsoft Sentinel, you need contributor or reader permissions on the resource group to which the workspace belongs.
- You might need additional permissions to connect specific data sources. You don't need additional permissions to connect to Defender for Cloud.
- Microsoft Sentinel is a paid service. For more information, refer to [Microsoft Sentinel pricing](#).

Enable Microsoft Sentinel

1. Sign into the Azure portal with a user that has contributor rights for **Defender for Cloud-Sentinelworkspace**.

2. Search for and select Microsoft Sentinel.

Microsoft Azure Microsoft Sentinel

All Services (5) Marketplace (11) Documentation (28) Azure Active Directory (30) Resources (0)

Resource Groups (0)

Services

-  Microsoft Sentinel
-  Microsoft Defender for Cloud
-  Microsoft Defender for IoT
-  Customer Lockbox for Microsoft Azure
-  Test Base for Microsoft 365

Marketplace

-  Microsoft Sentinel for SQL PaaS [Preview]
-  SOC 24*7 Monitoring with Microsoft Sentinel
-  Managed Microsoft Sentinel Service
-  Managed SIEM with Microsoft Sentinel
-  Adv Microsoft Sentinel XDR+SOC Managed Services
-  Microsoft Sentinel for Teams (Preview)
-  Microsoft Sentinel Training Lab Solution (Preview)
-  AMTRA Managed Microsoft Sentinel

3. Select Add.

4. On the **Microsoft Sentinel** blade, select **Defender for Cloud-Sentinelworkspace**.
 5. In Microsoft Sentinel, select **Data connectors** from the navigation menu.
 6. From the data connectors gallery, select **Microsoft Defender for Cloud**, and select the **Open connector page** button.

Microsoft Sentinel | Data Connectors

Search (Ctrl+F) Refresh

23 Connections 17 Connected 0 Coming soon

General Overview Log

Threat management Cases Dashboards Hunting Notebooks

Configuration News & guides Data connectors Analytics Playbooks Community Workspace settings

Search by name or provider PROVENDERS: All DATATYPES: All

STATUS	CONNECTOR NAME	LAST LOG RECEIVED
	Amazon Web Services	Amazon 06/27/19, 11:48 AM
	Azure Active Directory	Microsoft 07/03/19, 11:22 AM
	Azure Active Directory Identity Protection	Microsoft 07/03/19, 10:23 AM
	Azure Activity	Microsoft 07/03/19, 10:23 AM
	Azure Advanced Threat Protection	Microsoft 06/27/19, 11:16 PM
	Azure Information Protection	Microsoft 07/03/19, 11:22 AM
	Microsoft Defender for Cloud	Microsoft 06/27/19, 11:16 PM
	Barbaude Web Application Firewall	Barbaude 07/03/19, 08:38 AM
	Check Point	Check Point 06/18/19, 08:55 AM
	Cisco ASA	Cisco 07/03/19, 11:44 AM
	Common Event Format (CEF)	Any 07/03/19, 11:48 AM
	DNS	Microsoft 07/03/19, 11:21 AM
	F5	F5 07/03/19, 11:21 AM
	Fortinet	Fortinet 07/03/19, 11:21 AM

Azure Active Directory

Connected status Microsoft provider 32 minutes ago LAST LOG RECEIVED

DESCRIPTION

Get started with Azure Active Directory by connecting Audit and Sign-in logs to Azure Sentinel to gather insights around Azure Active Directory operations. You can learn about app usage, correlate findings across Azure Active Directory services, and review your Sign-in logs. You can get information on your 2558 usage. Azure Active Directory management activities like user, group, role, app management using our Audit log series.

LAST DATA RECEIVED 07/03/19, 11:22 AM

RELATED CONTENT 2 Dashboards (1) 2 Queries

DATA RECEIVED 24 SIGNINLOGS 7.97k AUDITLOGS

Go to log analytics

7.97k 303

DATATYPES

SigninLogs 07/03/19, 11:22 AM AuditLogs 07/03/19, 06:58 AM

Open connector page

7. Under **Configuration**, select **Connect** next to those subscriptions for which you want alerts to stream into Microsoft Sentinel. The **Connect** button will be available only if you have the required permissions and the Defender for Cloud subscription.
 8. You should now observe the **Connection Status** as **Connecting**. After connecting, it will switch to **Connected**.
 9. After confirming the connectivity, you can close Defender for Cloud **Data Connector** settings and refresh the page to observe alerts in Microsoft Sentinel. It might take some time for the logs to start syncing with Microsoft Sentinel. After you connect, you'll observe a data summary in the Data received graph and the connectivity status of the data types.
 10. You can select whether you want the alerts from Microsoft Defender for Cloud to automatically generate incidents in Microsoft Sentinel. Under **Create incidents**,

select **Enabled** to turn on the default analytics rule that automatically creates incidents from alerts. You can then edit this rule under **Analytics**, in the **Active rules** tab.

11. To use the relevant schema in Log Analytics for the Microsoft Defender for Cloud alerts, search for **SecurityAlert**.

One advantage of using Microsoft Sentinel as your SIEM is that it provides data correlation across multiple sources, which enables you to have an end-to-end visibility of your organization's security-related events.

Note

To learn how to increase visibility in your data and identify potential threats, refer to [Azure playbooks on TechNet Gallery](#), which has a collection of resources including a lab in which you can simulate attacks. You should not use this lab in a production environment.

To learn more about Microsoft Sentinel, refer to the following articles:

- [Quickstart](#): Get started with Microsoft Sentinel
- [Tutorial](#): Detect threats out-of-the-box

Next steps

Azure Monitor

- [Azure Monitor](#)

Microsoft Defender for Cloud

- [Microsoft Defender for Cloud](#)
- [Microsoft Defender for Cloud Smart Alert Correlation](#)
- [Microsoft Defender for Cloud Connect Data](#)
- [Microsoft Defender for Cloud Coverage](#)
- [Microsoft Defender for Cloud Endpoint Protection](#)
- [Microsoft Defender for Cloud FAQ](#)
- [Microsoft Defender for Cloud Planning](#)
- [Microsoft Defender for Cloud Secure Score](#)
- [Microsoft Defender for Cloud Security Alerts](#)
- [Microsoft Defender for Cloud Security Policies](#)

- Microsoft Defender for Cloud Security Recommendations
- Microsoft Defender for Cloud Supported Platforms
- Microsoft Defender for Cloud Threat Protection
- Microsoft Defender for Cloud Tutorial

Microsoft Sentinel

- Microsoft Sentinel
- Microsoft Sentinel Analytics
- Microsoft Sentinel Attack Detection
- Microsoft Sentinel Connect Windows Firewall
- Microsoft Sentinel Connect Windows Security Events
- Microsoft Sentinel Data Sources
- Microsoft Sentinel Hunting
- Microsoft Sentinel Investigate
- Microsoft Sentinel Monitor
- Microsoft Sentinel Overview
- Microsoft Sentinel Permissions
- Microsoft Sentinel Quickstart

Azure Stack

- Azure Stack
- Azure Stack Automate Onboarding PowerShell
- Azure Stack Hub

Related resources

- Implement a secure hybrid network
- Enhanced-security hybrid messaging infrastructure — web access
- Centralized app configuration and security
- Automate Sentinel integration with Azure DevOps

The MNIST database of handwritten digits

Article • 12/05/2023

The MNIST database of handwritten digits has a training set of 60,000 examples and a test set of 10,000 examples. The digits have been size-normalized and centered in a fixed-size image.

ⓘ Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

This dataset is sourced from [THE MNIST DATABASE of handwritten digits](#). It's a subset of the larger [NIST Hand-printed Forms and Characters Database](#) published by [National Institute of Standards and Technology](#).

Storage location

- Blob account: azureopendatastorage
- Container name: mnist

Four files are available in the container directly:

- train-images-idx3-ubyte.gz: training set images (9,912,422 bytes)
- train-labels-idx1-ubyte.gz: training set labels (28,881 bytes)
- t10k-images-idx3-ubyte.gz: test set images (1,648,877 bytes)
- t10k-labels-idx1-ubyte.gz: test set labels (4,542 bytes)

Data access

Azure Notebooks

Load MNIST into a data frame using Azure Machine Learning tabular datasets.

For more information on Azure Machine Learning datasets, see [Create Azure Machine Learning datasets](#).

Get complete dataset into a data frame

Python

```
from azureml.opendatasets import MNIST

mnist = MNIST.get_tabular_dataset()
mnist_df = mnist.to_pandas_dataframe()
mnist_df.info()
```

Get train and test data frames

Python

```
mnist_train = MNIST.get_tabular_dataset(dataset_filter='train')
mnist_train_df = mnist_train.to_pandas_dataframe()
X_train = mnist_train_df.drop("label", axis=1).astype(int).values/255.0
y_train = mnist_train_df.filter(items=["label"]).astype(int).values

mnist_test = MNIST.get_tabular_dataset(dataset_filter='test')
mnist_test_df = mnist_test.to_pandas_dataframe()
X_test = mnist_test_df.drop("label", axis=1).astype(int).values/255.0
y_test = mnist_test_df.filter(items=[ "label" ]).astype(int).values
```

Plot some images of the digits

Python

```
%matplotlib inline
import numpy as np
import matplotlib.pyplot as plt

# now let's show some randomly chosen images from the training set.
count = 0
sample_size = 30
```

```
plt.figure(figsize=(16, 6))
for i in np.random.permutation(X_train.shape[0])[:sample_size]:
    count = count + 1
    plt.subplot(1, sample_size, count)
    plt.axhline(' ')
    plt.axvline(' ')
    plt.text(x=10, y=-10, s=y_train[i], fontsize=18)
    plt.imshow(X_train[i].reshape(28, 28), cmap=plt.cm.Greys)
plt.show()
```

Download or mount MNIST raw files Azure Machine Learning file datasets.

This works only for Linux based compute. For more information on Azure Machine Learning datasets, see [Create Azure Machine Learning datasets](#).

Python

```
mnist_file = MNIST.get_file_dataset()
mnist_file
```

Python

```
mnist_file.to_path()
```

Download files to local storage

Python

```
import os
import tempfile

data_folder = tempfile.mkdtemp()
data_paths = mnist_file.download(data_folder, overwrite=True)
data_paths
```

Mount files. Useful when training job will run on a remote compute.

Python

```
import gzip
import struct
import pandas as pd
```

```
import numpy as np

# load compressed MNIST gz files and return pandas dataframe of numpy
arrays
def load_data(filename, label=False):
    with gzip.open(filename) as gz:
        gz.read(4)
        n_items = struct.unpack('>I', gz.read(4))
        if not label:
            n_rows = struct.unpack('>I', gz.read(4))[0]
            n_cols = struct.unpack('>I', gz.read(4))[0]
            res = np.frombuffer(gz.read(n_items[0] * n_rows * n_cols),
            dtype=np.uint8)
            res = res.reshape(n_items[0], n_rows * n_cols)
        else:
            res = np.frombuffer(gz.read(n_items[0]), dtype=np.uint8)
            res = res.reshape(n_items[0], 1)
    return pd.DataFrame(res)
```

Python

```
import sys
mount_point = tempfile.mkdtemp()
print(mount_point)
print(os.path.exists(mount_point))

if sys.platform == 'linux':
    print("start mounting....")
    with mnist_file.mount(mount_point):
        print("list dir...")
        print(os.listdir(mount_point))
        print("get the dataframe info of mounted data...")
        train_images_df = load_data(next(path for path in data_paths if
path.endswith("train-images-idx3-ubyte.gz")))
        print(train_images_df.info())
```

Azure Databricks

azureml-opendatasets

Load MNIST into a data frame using Azure Machine Learning tabular datasets.

For more information on Azure Machine Learning datasets, see [Create Azure Machine Learning datasets](#).

Get complete dataset into a data frame

Python

```
# This is a package in preview.
from azureml.opendatasets import MNIST

mnist = MNIST.get_tabular_dataset()
mnist_df = mnist.to_spark_dataframe()
```

Python

```
display(mnist_df.limit(5))
```

Download or mount MNIST raw files Azure Machine Learning file datasets.

This works only for Linux based compute. For more information on Azure Machine Learning datasets, see [Create Azure Machine Learning datasets](#).

Python

```
mnist_file = MNIST.get_file_dataset()
mnist_file
```

Python

```
mnist_file.to_path()
```

Download files to local storage

Python

```
import os
import tempfile

mount_point = tempfile.mkdtemp()
mnist_file.download(mount_point, overwrite=True)
```

Mount files. Useful when training job will run on a remote compute.

Python

```
import gzip
import struct
import pandas as pd
import numpy as np

# load compressed MNIST gz files and return numpy arrays
def load_data(filename, label=False):
    with gzip.open(filename) as gz:
        gz.read(4)
        n_items = struct.unpack('>I', gz.read(4))
        if not label:
            n_rows = struct.unpack('>I', gz.read(4))[0]
            n_cols = struct.unpack('>I', gz.read(4))[0]
            res = np.frombuffer(gz.read(n_items[0] * n_rows * n_cols),
            dtype=np.uint8)
            res = res.reshape(n_items[0], n_rows * n_cols)
        else:
            res = np.frombuffer(gz.read(n_items[0]), dtype=np.uint8)
            res = res.reshape(n_items[0], 1)
    return pd.DataFrame(res)
```

Python

```
import sys
mount_point = tempfile.mkdtemp()
print(mount_point)
print(os.path.exists(mount_point))
print(os.listdir(mount_point))

if sys.platform == 'linux':
    print("start mounting....")
    with mnist_file.mount(mount_point):
        print(context.mount_point )
        print(os.listdir(mount_point))
        train_images_df = load_data(os.path.join(mount_point, 'train-images-
idx3-ubyte.gz'))
        print(train_images_df.info())
```

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

Public Holidays

Article • 12/05/2023

Worldwide public holiday data sourced from PyPI holidays package and Wikipedia, covering 38 countries or regions from 1970 to 2099.

Each row indicates the holiday info for a specific date, country or region, and whether most people have paid time off.

ⓘ Note

Microsoft provides Azure Open Datasets on an “as is” basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Volume and retention

This dataset is stored in Parquet format. It's a snapshot with holiday information from January 1, 1970 to January 1, 2099. The data size is about 500KB.

Storage location

This dataset is stored in the East US Azure region. We recommend locating compute resources in East US for affinity.

Additional information

This dataset combines data sourced from [Wikipedia \(WikiMedia Foundation Inc\)](#) and [PyPI holidays package](#).

- Wikipedia: [original source](#), [original license](#)
- PyPI holidays: [original source](#), [original license](#)

The combined dataset is provided under the [Creative Commons Attribution-ShareAlike 3.0 Unported License](#).

Email aod@microsoft.com if you have any questions about the data source.

Columns

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

Name	Data type	Unique	Values (sample)	Description
countryOrRegion	string	38	Sweden Norway	Country or region full name.
countryRegionCode	string	35	SE NO	Country or region code following the format here.
date	timestamp	20,665	2074-01-01 00:00:00 2025-12-25 00:00:00	Date of the holiday.
holidayName	string	483	Søndag Söndag	Full name of the holiday.
isPaidTimeOff	boolean	3	True	Indicate whether most people have paid time off on this date (only available for US, GB, and India now). If it is NULL, it means unknown.
normalizeHolidayName	string	438	Søndag Söndag	Normalized name of the holiday.

Preview

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

countryOrRegion	holidayName	normalizeHolidayName	countryRegionCode	date
Norway	Søndag	Søndag	NO	12/28/2098 12:00:00 AM
Sweden	Søndag	Söndag	SE	12/28/2098 12:00:00

countryOrRegion	holidayName	normalizeHolidayName	countryRegionCode	date
				AM
Australia	Boxing Day	Boxing Day	AU	12/26/2098 12:00:00 AM
Hungary	Karácsony másnapja	Karácsony másnapja	HU	12/26/2098 12:00:00 AM
Austria	Stefanitag	Stefanitag	AT	12/26/2098 12:00:00 AM
Canada	Boxing Day	Boxing Day	CA	12/26/2098 12:00:00 AM
Croatia	Sveti Stjepan	Sveti Stjepan	HR	12/26/2098 12:00:00 AM
Czech	2. svátek vánoční	2. svátek vánoční	CZ	12/26/2098 12:00:00 AM

Data access

Azure Notebooks

azureml-opendatasets

```
# This is a package in preview.
from azureml.opendatasets import PublicHolidays

from datetime import datetime
from dateutil import parser
from dateutil.relativedelta import relativedelta

end_date = datetime.today()
start_date = datetime.today() - relativedelta(months=1)
```

```
hol = PublicHolidays(start_date=start_date, end_date=end_date)
hol_df = hol.to_pandas_dataframe()
```

```
hol_df.info()
```

Azure Databricks

azureml-opendatasets

```
# This is a package in preview.
# You need to pip install azureml-opendatasets in Databricks cluster.
https://learn.microsoft.com/azure/data-explorer/connect-from-databricks#install-the-python-library-on-your-azure-databricks-cluster
from azureml.opendatasets import PublicHolidays
```

```
from datetime import datetime
from dateutil import parser
from dateutil.relativedelta import relativedelta
```

```
end_date = datetime.today()
start_date = datetime.today() - relativedelta(months=1)
hol = PublicHolidays(start_date=start_date, end_date=end_date)
hol_df = hol.to_spark_dataframe()
```

```
display(hol_df.limit(5))
```

Azure Synapse

azureml-opendatasets

Python

```
# This is a package in preview.
from azureml.opendatasets import PublicHolidays

from datetime import datetime
```

```
from dateutil import parser
from dateutil.relativedelta import relativedelta

end_date = datetime.today()
start_date = datetime.today() - relativedelta(months=1)
hol = PublicHolidays(start_date=start_date, end_date=end_date)
hol_df = hol.to_spark_dataframe()
```

Python

```
# Display top 5 rows
display(hol_df.limit(5))
```

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

Boston Safety Data

Article • 12/05/2023

311 calls reported to the city of Boston.

Refer to this link to learn more about [BOS:311](#).

ⓘ Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Volume and retention

This dataset is stored in Parquet format. It is updated daily, and contains about 100-K rows (10 MB) in total as of 2019.

This dataset contains historical records accumulated from 2011 to the present. You can use parameter settings in our SDK to fetch data within a specific time range.

Storage location

This dataset is stored in the East US Azure region. Allocating compute resources in East US is recommended for affinity.

Additional information

This dataset is sourced from city of Boston government. For more information, see [Boston's dataset site](#). For dataset licensing, see [Open Data Commons Public Domain Dedication and License \(ODC PDDL\)](#).

Columns

ⓘ [Expand table](#)

Name	Data type	Unique	Values (sample)	Description
address	string	140,612	" " 1 City Hall Plz Boston MA 02108	Location.
category	string	54	Street Cleaning Sanitation	Reason of the service request.
dataSubtype	string	1	311_All	"311_All"
dataType	string	1	Safety	"Safety"
dateTime	timestamp	1,529,075	2015-07-23 10:51:00 2015-07-23 10:47:00	Open date and time of the service request.
latitude	double	1,622	42.3594 42.3603	This is the latitude value. Lines of latitude are parallel to the equator.
longitude	double	1,806	-71.0587 -71.0583	This is the longitude value. Lines of longitude run perpendicular to lines of latitude, and all pass through both poles.
source	string	7	Constituent Call Citizens Connect App	Original source of the case.
status	string	2	Closed Open	Case status.
subcategory	string	209	Parking Enforcement Requests for Street Cleaning	Type of the service request.

Preview

[Expand table](#)

dataType	dataSubtype	dateTime	category	subcategory	status	address	latitude	longitude	source	extendedProperties
Safety	311_All	4/27/2021 11:45:49 PM	Enforcement & Abandoned Vehicles	Parking Enforcement	Open	51 Gardner St Allston MA 02134	42.3535	-71.1285	Citizens Connect App	
Safety	311_All	4/27/2021 11:43:43 PM	Sanitation	Missed Trash/Recycling/Yard Waste/Bulk Item	Open	4 Putnam Pl Roxbury MA 02119	42.3298	-71.0883	Self Service	
Safety	311_All	4/27/2021 11:37:19 PM	Enforcement & Abandoned Vehicles	Parking Enforcement	Open	36 Raven St Dorchester MA 02125	42.3177	-71.0546	Citizens Connect App	
Safety	311_All	4/27/2021 11:30:00 PM	Sanitation	Missed Trash/Recycling/Yard Waste/Bulk Item	Open	58 Bicknell St Dorchester MA 02121	42.2984	-71.0834	Constituent Call	
Safety	311_All	4/27/2021 11:10:20 PM	Enforcement & Abandoned Vehicles	Parking Enforcement	Open	2000 Commonwealth Ave Brighton MA 02135	42.3394	-71.1585	Citizens Connect App	
Safety	311_All	4/27/2021 11:06:00 PM	Noise Disturbance	Loud Parties/Music/People	Open	INTERSECTION of Lewis St & North St Boston MA	42.3594	-71.0587	Constituent Call	
Safety	311_All	4/27/2021 11:05:00 PM	Enforcement & Abandoned Vehicles	Parking Enforcement	Open	1 Nassau St Boston MA 02111	42.3486	-71.0629	Constituent Call	
Safety	311_All	4/27/2021 11:00:55 PM	Code Enforcement	Poor Conditions of Property	Open	17 Mercer St South Boston MA 02127	42.3332	-71.0492	Citizens Connect App	

Data access

Azure Notebooks

```
azureml-opendatasets

# This is a package in preview.
from azureml.opendatasets import BostonSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = BostonSafety(start_date=start_date, end_date=end_date)
safety = safety.to_pandas_dataframe()

safety.info()
```

Azure Databricks

```
azureml-opendatasets
```

```
# This is a package in preview.
# You need to pip install azureml-opendatasets in Databricks cluster. https://learn.microsoft.com/azure/data-explorer/connect-from-databricks#install-the-python-library-on-your-azure-databricks-cluster
from azureml.opendatasets import BostonSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = BostonSafety(start_date=start_date, end_date=end_date)
safety = safety.to_spark_dataframe()
```

```
display(safety)
```

Azure Synapse

azureml-opendatasets

Python

```
from azureml.opendatasets import BostonSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = BostonSafety(start_date=start_date, end_date=end_date)
safety = safety.to_spark_dataframe()
```

Python

```
display(safety)
```

Examples

- See the [City Safety Analytics](#) example on GitHub.

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

Chicago Safety Data

Article • 12/05/2023

311 service requests from the city of Chicago, including historical sanitation code complaints, pot holes reported, and street light issues

All open sanitation code complaints made to 311 and all requests completed since January 1, 2011. The Department of Streets and Sanitation investigates and remedies reported violations of Chicago's sanitation code. Residents may request service for violations such as overflowing dumpsters and garbage in the alley. 311 sometimes receives duplicate sanitation code complaints. Requests that have been labeled as duplicates are in the same geographic area as a previous request and have been entered into 311's Customer Service Request (CSR) system at around the same time. Duplicate complaints are labeled as such in the status field, as either "Open - Dup" or "Completed - Dup."

Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

The Chicago Department of Transportation (CDOT) oversees the patching of potholes on over 4,000 miles of arterial and residential streets in Chicago. CDOT receives reports of potholes through the 311 call center. CDOT uses a mapping and tracking system to identify pothole locations and schedule crews.

One call to 311 can generate multiple pothole repairs. When a crew arrives to repair a 311 pothole, it fills all the other potholes within the block. Pothole repairs are completed within seven days from the first report of a pothole to 311. Weather conditions, frigid temps, and precipitation, influence how long a repair takes. On days when weather is cooperative and there's no precipitation, crews can fill several thousand potholes.

If a previous request is already open for a buffer of four addresses, the request is given the status of "Duplicate (Open)". For example, if there's an existing CSR for 6535 N Western and a new request is received for 6531 N Western (which is within four addresses of the original CSR) then the new request is given a status of "Duplicate (Open)". Once the street is repaired, the status in CSR will read "Completed" for the original request and "Duplicate (Closed)" for any duplicate requests. A service request also receives the status of "Completed" when the reported address is inspected but no potholes are found or have already been filled. If another issue is found with the street, such as a "cave-in" or "failed utility cut", then it's directed to the appropriate department or contractor.

All open reports of "Street Lights - All Out" (an outage of three or more lights) made to 311 and all requests completed since January 1, 2011. The Chicago Department of Transportation (CDOT) oversees approximately 250,000 street lights that illuminate arterial and residential streets in Chicago. CDOT performs repairs and bulb replacements in response to residents' reports of street light outages. Whenever CDOT receives a report of an "All Out" the electrician assigned to make the repair looks at the lights in that circuit (each circuit has 8-16 lights) to make sure they're working properly. If a second request of lights out in the same circuit is made within four calendar days of the original request, the newest request is automatically given the status of "Duplicate (Open)." Since CDOT's electrician will be looking at the lights in a circuit to verify they're working, any "Duplicate (Open)" address will automatically be observed and repaired. Once the street lights are repaired, the status in CSR will read "Completed" for the original request and "Duplicate (Closed)" for any duplicate requests. A service request also receives the status of "Completed" when the reported lights are inspected but found to be in good repair and functioning; when the service request is for a non-existent address; or when the lights are maintained by a contractor. Data is updated daily.

Volume and retention

This dataset is stored in Parquet format. It is updated daily, and contains about 1M rows (80 MB) in total as of 2018.

This dataset contains historical records accumulated from 2011 to 2018. You can use parameter settings in our SDK to fetch data within a specific time range.

Storage location

This dataset is stored in the East US Azure region. Allocating compute resources in East US is recommended for affinity.

Related datasets

- [Chicago sanitation ↗](#)
- [Chicago pot holes ↗](#)
- [Chicago street lights ↗](#)

Additional information

This dataset is sourced from city of Chicago government.

Reference here for the terms of using this dataset. Email dataportal@cityofchicago.org if you have any questions about the data source.

Columns

 [Expand table](#)

Name	Data type	Unique	Values (sample)	Description
address	string	140,612	" " 1 City Hall Plz Boston MA 02108	Location.
category	string	54	Street Cleaning Sanitation	Reason of the service request.
dataSubtype	string	1	311_All	"311_All"
dataType	string	1	Safety	"Safety"
dateTime	timestamp	1,529,075	2015-07-23 10:51:00 2015-07-23 10:47:00	Open date and time of the service request.
latitude	double	1,622	42.3594 42.3603	This is the latitude value. Lines of latitude are parallel to the equator.
longitude	double	1,806	-71.0587 -71.0583	This is the longitude value. Lines of longitude run perpendicular to lines of latitude, and all pass through both poles.
source	string	7	Constituent Call Citizens Connect App	Original source of the case.
status	string	2	Closed Open	Case status.
subcategory	string	209	Parking Enforcement Requests for Street Cleaning	Type of the service request.

Preview

 [Expand table](#)

dataType	dataSubtype	dateTime	category	subcategory	status	address	latitude	longitude	source	extendedProperties
Safety	311_All	4/25/2021 11:55:04 PM	Street Light Out Complaint	null	Open	4800 W WASHINGTON BLVD	41.882148426	-87.74556256	null	
Safety	311_All	4/25/2021 11:54:31 PM	311 INFORMATION ONLY CALL	null	Completed	2111 W Lexington ST			null	
Safety	311_All	4/25/2021 11:52:11 PM	311 INFORMATION ONLY CALL	null	Completed	2111 W Lexington ST			null	
Safety	311_All	4/25/2021 11:49:56 PM	311 INFORMATION ONLY CALL	null	Completed	2111 W Lexington ST			null	
Safety	311_All	4/25/2021 11:48:53 PM	Garbage Cart Maintenance	null	Open	3409 E 106TH ST	41.702545562	-87.540917602	null	
Safety	311_All	4/25/2021 11:46:01 PM	311 INFORMATION ONLY CALL	null	Completed	2111 W Lexington ST			null	
Safety	311_All	4/25/2021 11:45:46	Aircraft Noise Complaint	null	Completed	10510 W ZEMKE RD			null	

dataType	dataSubtype	PM	dateTime	category	subcategory	status	address	latitude	longitude	source	extendedProperties
Safety	311_All		4/25/2021 11:45:02 PM	311 INFORMATION ONLY CALL	null	Completed	2111 W Lexington ST			null	
Safety	311_All		4/25/2021 11:44:24 PM	Sewer Cave-In Inspection Request	null	Open	7246 W THORNDALE AVE	41.987984339	-87.808702917	null	

Data access

Azure Notebooks

```
azureml-opendatasets
```

```
# This is a package in preview.
from azureml.opendatasets import ChicagoSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = ChicagoSafety(start_date=start_date, end_date=end_date)
safety = safety.to_pandas_dataframe()
```

```
safety.info()
```

Azure Databricks

```
azureml-opendatasets
```

```
# This is a package in preview.
# You need to pip install azureml-opendatasets in Databricks cluster. https://learn.microsoft.com/azure/data-explorer/connect-from-databricks#install-the-python-library-on-your-azure-databricks-cluster
from azureml.opendatasets import ChicagoSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = ChicagoSafety(start_date=start_date, end_date=end_date)
safety = safety.to_spark_dataframe()
```

```
display(safety.limit(5))
```

Azure Synapse

```
azureml-opendatasets
```

```
Python
```

```
# This is a package in preview.
from azureml.opendatasets import ChicagoSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = ChicagoSafety(start_date=start_date, end_date=end_date)
safety = safety.to_spark_dataframe()
```

Python

```
# Display top 5 rows
display(safety.limit(5))
```

Python

```
# Display data statistic information
display(safety, summary = True)
```

Examples

- See the [City Safety Analytics](#) example on GitHub.

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

New York City Safety Data

Article • 12/05/2023

All New York City 311 service requests from 2010 to the present.

ⓘ Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Volume and retention

This dataset is stored in Parquet format. It is updated daily, and contains about 12M rows (500 MB) in total as of 2019.

This dataset contains historical records accumulated from 2010 to the present. You can use parameter settings in our SDK to fetch data within a specific time range.

Storage location

This dataset is stored in the East US Azure region. Allocating compute resources in East US is recommended for affinity.

Additional information

This dataset is sourced from New York City government, for more information, see the [City of New York website](#). See the [terms of this dataset](#).

Columns

[Expand table](#)

Name	Data type	Unique	Values (sample)	Description
address	string	1,536,593	655 EAST 230 STREET 78-15 PARSONS BOULEVARD	House number of incident address provided by submitter.
category	string	446	Noise - Residential HEAT/HOT WATER	This is the first level of a hierarchy identifying the topic of the incident or condition (Complaint Type). It may have a corresponding subcategory (Descriptor) or may stand alone.
dataSubtype	string	1	311_All	"311_All"
dataType	string	1	Safety	"Safety"
dateTime	timestamp	17,332,609	2013-01-24 00:00:00 2015-01-08 00:00:00	Date Service Request was created.
latitude	double	1,513,691	40.89187241649303 40.72195913199264	Geo based Latitude of the incident location.
longitude	double	1,513,713	-73.86016845296459 -73.80969682426189	Geo based Longitude of the incident location.
status	string	13	Closed Pending	Status of Service Request submitted.
subcategory	string	1,716	Loud Music/Party ENTIRE BUILDING	This is associated to the category (Complaint Type), and provides further detail on the incident or condition. Its values are dependent on the Complaint Type, and are not always required in Service Request.

Preview

[Expand table](#)

dataType	dataSubtype	dateTime	category	subcategory	status	address	latitude	longitude	source	exten
Safety	311_All	4/25/2021 2:05:05 AM	Noise - Street/Sidewalk	Loud Music/Party	In Progress	2766 BATH AVENUE	40.5906129741766	-73.9847949011337	null	
Safety	311_All	4/25/2021 2:04:33 AM	Noise - Commercial	Loud Music/Party	In Progress	1033 WEBSTER AVENUE	40.8285784533256	-73.9117746958432	null	
Safety	311_All	4/25/2021 2:04:27 AM	Noise - Residential	Loud Music/Party	In Progress	620 WEST 141 STREET	40.8241726554395	-73.9530069547366	null	
Safety	311_All	4/25/2021 2:04:04 AM	Noise - Residential	Loud Music/Party	In Progress	1647 64 STREET	40.6218907202382	-73.9931125332078	null	
Safety	311_All	4/25/2021 2:04:01 AM	Noise - Residential	Loud Music/Party	In Progress	30 LENOX AVENUE	40.7991622274945	-73.9517496365803	null	
Safety	311_All	4/25/2021 2:03:40 AM	Illegal Parking	Double Parked Blocking Traffic	In Progress	304 WEST 148 STREET	40.8248229687124	-73.940696262361	null	
Safety	311_All	4/25/2021 2:03:31 AM	Noise - Street/Sidewalk	Loud Music/Party	In Progress	ADEE AVENUE	40.8708386263454	-73.8382363208686	null	
Safety	311_All	4/25/2021 2:03:18 AM	Noise - Residential	Loud Music/Party	In Progress	340 EVERGREEN AVENUE	40.6947512704197	-73.9248330229197	null	
Safety	311_All	4/25/2021 2:03:13 AM	Noise - Residential	Banging/Pounding	In Progress	25 REMSEN STREET	40.6948938116483	-73.9973494607802	null	

Data access

Azure Notebooks

```
azureml-opendatasets

# This is a package in preview.
from azureml.opendatasets import SanFranciscoSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = SanFranciscoSafety(start_date=start_date, end_date=end_date)
safety = safety.to_pandas_dataframe()

safety.info()
```

Azure Databricks

```
azureml-opendatasets
```

```
# This is a package in preview.
# You need to pip install azureml-opendatasets in Databricks cluster. https://learn.microsoft.com/azure/data-explorer/connect-from-databricks#install-the-python-library-on-your-azure-databricks-cluster
from azureml.opendatasets import SanFranciscoSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = SanFranciscoSafety(start_date=start_date, end_date=end_date)
safety = safety.to_spark_dataframe()
```

```
display(safety.limit(5))
```

Azure Synapse

azureml-opendatasets

Python

```
# This is a package in preview.
from azureml.opendatasets import SanFranciscoSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = SanFranciscoSafety(start_date=start_date, end_date=end_date)
safety = safety.to_spark_dataframe()
```

Python

```
# Display top 5 rows
display(safety.limit(5))
```

Examples

- See the [City Safety Analytics](#) example on GitHub.

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

San Francisco Safety Data

Article • 12/05/2023

Fire department calls for service and 311 cases in San Francisco.

ⓘ Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Fire Calls-For-Service includes all fire unit responses to calls. Each record includes the call number, incident number, address, unit identifier, call type, and disposition. All relevant time intervals are also included. Because this dataset is based on responses, and since most calls involved multiple units, there are multiple records for each call number. Addresses are associated with a block number, intersection, or call box, not a specific address.

311 Cases include cases associated with a place or thing (for example parks, streets, or buildings) and created after July 1, 2008. Cases that are logged by a user about their own needs are excluded. For example, property or business tax questions, parking permit requests, and so on. For more information, see the [Program Link](#).

Volume and retention

This dataset is stored in Parquet format. It is updated daily with about 6M rows (400 MB) as of 2019.

This dataset contains historical records accumulated from 2015 to the present. You can use parameter settings in our SDK to fetch data within a specific time range.

Storage location

This dataset is stored in the East US Azure region. Allocating compute resources in East US is recommended for affinity.

Related datasets

- [Fire Department Calls](#)
- [311 Cases](#)

Columns

[Expand table](#)

Name	Data type	Unique	Values (sample)	Description
address	string	280,652	Not associated with a specific address 0 Block of 6TH ST	Address of incident (note: address and location generalized to mid-block of street, intersection, or nearest call box location, to protect caller privacy).
category	string	108	Street and Sidewalk Cleaning Potentially Life-Threatening	The human readable name of the 311 service request type or call type group for 911 fire calls.
dataSubtype	string	2	911_Fire 311_All	"911_Fire" or "311_All".
dataType	string	1	Safety	"Safety"
dateTime	timestamp	6,496,563	2020-10-19 12:28:08 2020-07-28 06:40:26	The date and time when the service request was made or when the fire call was received.
latitude	double	1,615,369	37.777624238929 37.786117211838	Latitude of the location, using the WGS84 projection.
longitude	double	1,554,612	-122.39998111124 -122.419854245692	Longitude of the location, using the WGS84 projection.
source	string	9	Phone Mobile/Open311	Mechanism or path by which the service request was received; typically "Phone", "Text/SMS", "Website", "Mobile App", "Twitter", etc. but terms may

Name	Data type	Unique	Values (sample)	Description					
				vary by system.					
status	string	3	Closed Open	A single-word indicator of the current state of the service request. (Note: GeoReport V2 only permits "open" and "closed")					
subcategory	string	1,270	Medical Incident Bulky Items	The human readable name of the service request subtype for 311 cases or call type for 911 fire calls.					

Preview

[Expand table](#)

dataType	dataSubtype	dateTime	category	subcategory	status	address	latitude	longitude	source	extendedProperty
Safety	911_Fire	4/26/2021 2:56:13 AM	Non Life-threatening	Medical Incident	null	700 Block of GEARY ST	37.7863607914647	-122.415616900246	null	
Safety	911_Fire	4/26/2021 2:56:13 AM	Non Life-threatening	Medical Incident	null	700 Block of GEARY ST	37.7863607914647	-122.415616900246	null	
Safety	911_Fire	4/26/2021 2:54:03 AM	Non Life-threatening	Medical Incident	null	0 Block of ESSEX ST	37.7860048266229	-122.395077258809	null	
Safety	911_Fire	4/26/2021 2:54:03 AM	Non Life-threatening	Medical Incident	null	0 Block of ESSEX ST	37.7860048266229	-122.395077258809	null	
Safety	911_Fire	4/26/2021 2:52:17 AM	Non Life-threatening	Medical Incident	null	700 Block of 29TH AVE	37.7751770865322	-122.488604397217	null	
Safety	911_Fire	4/26/2021 2:50:28 AM	Potentially Life-Threatening	Medical Incident	null	1000 Block of GEARY ST	37.7857350982044	-122.420555240691	null	
Safety	911_Fire	4/26/2021 2:50:28 AM	Potentially Life-Threatening	Medical Incident	null	1000 Block of GEARY ST	37.7857350982044	-122.420555240691	null	
Safety	911_Fire	4/26/2021 2:33:52 AM	Non Life-threatening	Medical Incident	null	100 Block of BELVEDERE ST	37.767791696654	-122.449332294394	null	
Safety	911_Fire	4/26/2021 2:33:52 AM	Non Life-threatening	Medical Incident	null	100 Block of BELVEDERE ST	37.767791696654	-122.449332294394	null	
Safety	911_Fire	4/26/2021 2:33:51 AM	Potentially Life-Threatening	Medical Incident	null	100 Block of 6TH ST	37.7807920802756	-122.408385745499	null	

Data access

Azure Notebooks

```
azureml-opendatasets

# This is a package in preview.
from azureml.opendatasets import NycSafety

from datetime import datetime
from dateutil import parser
```

```
end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = NycSafety(start_date=start_date, end_date=end_date)
safety = safety.to_pandas_dataframe()
```

```
safety.info()
```

Azure Databricks

azureml-opendatasets

```
# This is a package in preview.
# You need to pip install azureml-opendatasets in Databricks cluster. https://learn.microsoft.com/azure/data-explorer/connect-from-databricks#install-the-python-library-on-your-azure-databricks-cluster
from azureml.opendatasets import NycSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = NycSafety(start_date=start_date, end_date=end_date)
safety = safety.to_spark_dataframe()
```

```
display(safety.limit(5))
```

Azure Synapse

azureml-opendatasets

```
Python

# This is a package in preview.
from azureml.opendatasets import NycSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = NycSafety(start_date=start_date, end_date=end_date)
safety = safety.to_spark_dataframe()
```

Python

```
# Display top 5 rows
display(safety.limit(5))
```

Examples

- See the [City Safety Analytics](#) example on GitHub.

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

Seattle Safety Data

Article • 12/05/2023

Seattle Fire Department 911 dispatches.

ⓘ Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Volume and retention

This dataset is stored in Parquet format. It's updated daily, and contains about 800,000 rows (20 MB) in 2019.

This dataset contains historical records accumulated from 2010 to the present. You can use parameter settings in our SDK to fetch data within a specific time range.

Storage location

This dataset is stored in the East US Azure region. We recommend locating compute resources in East US for affinity.

Additional information

This dataset is sourced from city of Seattle government. For more information, see the [city of Seattle website](#). View the [Licensing and Attribution for the terms of using this dataset](#). Email open.data@seattle.gov if you have any questions about the data source.

Columns

 [Expand table](#)

Name	Data type	Unique	Values (sample)	Description
address	string	196,965	517 3rd Av 318 2nd Av Et S	Location of Incident.
category	string	232	Aid Response Medic Response	Response Type.
dataSubtype	string	1	911_Fire	"911_Fire"
dataType	string	1	Safety	"Safety"
dateTime	timestamp	1,533,401	2020-11-04 06:49:00 2019-06-19 13:49:00	The date and time of the call.
latitude	double	94,332	47.602172 47.600194	This is the latitude value. Lines of latitude are parallel to the equator.
longitude	double	79,492	-122.330863 -122.330541	This is the longitude value. Lines of longitude run perpendicular to lines of latitude, and all pass through both poles.

Preview

[Expand table](#)

dataType	dataSubtype	dateTime	category	subcategory	status	address	latitude	longitude	source	extendedProperties
Safety	911_Fire	4/28/2021 5:22:00 AM	Rubbish Fire	null	null	200 University St	47.607299	-122.337087	null	
Safety	911_Fire	4/28/2021 5:15:00 AM	Triaged Incident	null	null	6th Ave / Olive Way	47.61313	-122.336282	null	
Safety	911_Fire	4/28/2021 5:12:00 AM	Aid Response	null	null	4th Ave S / Seattle Blvd S	47.596486	-122.329046	null	
Safety	911_Fire	4/28/2021 5:09:00 AM	Rubbish Fire	null	null	3rd Ave / University St	47.607763	-122.335976	null	
Safety	911_Fire	4/28/2021 4:57:00 AM	Low Acuity Response	null	null	533 3rd Ave W	47.623717	-122.360635	null	
Safety	911_Fire	4/28/2021 4:57:00 AM	Trans to AMR	null	null	4638 S Austin St	47.534702	-122.274812	null	
Safety	911_Fire	4/28/2021 4:55:00 AM	Triaged Incident	null	null	8th Ave N / Harrison St	47.622051	-122.341066	null	

Data access

Azure Notebooks

azureml-opendatasets

```
# This is a package in preview.
from azureml.opendatasets import SeattleSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = SeattleSafety(start_date=start_date, end_date=end_date)
safety = safety.to_pandas_dataframe()
```

```
safety.info()
```

Azure Databricks

azureml-opendatasets



```
# This is a package in preview.
# You need to pip install azureml-opendatasets in Databricks cluster.
https://learn.microsoft.com/azure/data-explorer/connect-from-databricks#install-the-python-library-on-
your-azure-databricks-cluster
from azureml.opendatasets import SeattleSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = SeattleSafety(start_date=start_date, end_date=end_date)
safety = safety.to_spark_dataframe()
```

```
display(safety.limit(5))
```

Azure Synapse

azureml-opendatasets

Python

```
# This is a package in preview.
from azureml.opendatasets import SeattleSafety

from datetime import datetime
from dateutil import parser

end_date = parser.parse('2016-01-01')
start_date = parser.parse('2015-05-01')
safety = SeattleSafety(start_date=start_date, end_date=end_date)
safety = safety.to_spark_dataframe()
```

Python

```
# Display top 5 rows
display(safety.limit(5))
```

Examples

- See the [City Safety Analytics](#) example on GitHub.

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

US Labor Force Statistics

Article • 12/05/2023

Labor Force Statistics labor force, labor force participation rates, and the civilian noninstitutional population by age, gender, race, and ethnic groups. in the United States.

This dataset is sourced from [Current Employment Statistics - CES \(National\) data](#) published by [US Bureau of Labor Statistics \(BLS\)](#). Review [Linking and Copyright Information](#) and [Important Web Site Notices](#) for the terms and conditions related to the use this dataset.

ⓘ Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Storage location

This dataset is stored in the East US Azure region. Allocating compute resources in East US is recommended for affinity.

Related datasets

- [US National Employment Hours and Earnings](#)
- [US State Employment Hours and Earnings](#)
- [US Local Area Unemployment Statistics](#)

Columns

ⓘ [Expand table](#)

Name	Data type	Unique	Values (sample)
absn_code	int	4	3 4
activity_code	int	7	8 3
ages_code	int	35	10 17
born_code	int	3	1 2
cert_code	int	5	4 3
chld_code	int	6	2 5
class_code	int	14	2 1
disa_code	int	3	2 1
duration_code	int	11	18 6
education_code	int	9	40 19
entr_code	int	3	1 2
expr_code	int	3	1 2
footnote_codes	string	7	nan 4.0
hheader_code	int	2	1
hour_code	int	13	1 16
indy_code	int	323	368 169
jdes_code	int	3	1 2

Name	Data type	Unique	Values (sample)
lfst_code	int	33	20 30
look_code	int	7	1 6
mari_code	int	5	2 1
mjhs_code	int	6	1 5
occupation_code	int	566	8999 4999
orig_code	int	14	1 2
pcts_code	int	23	5 8
period	string	18	M07 M06
periodicity_code	string	3	M Q
race_code	int	14	1 3
rjnw_code	int	9	1 3
rnlf_code	int	11	63 64
rwns_code	int	17	10 1
seasonal	string	2	U S
seek_code	int	2	1
series_id	string	45,478	LNU01300000 LNU02034560
series_title	string	34,264	(Unadj) Employment Level - Agriculture and Related Industries (Unadj) Civilian Labor Force Level
sexs_code	int	3	1 2
tdat_code	int	6	1 4
value	float	121,742	3.0 4.0
vets_code	int	8	25 1
wkst_code	int	7	1 4
year	int	80	2018 2017

Preview

[Expand table](#)

series_id	year	period	value	footnote_codes	lfst_code	periodicity_code	series_title	absn_code	activity_code	ages_code	cert_code	c
LNS11000031Q	1972	Q01	4300	nan	10	Q	(Seas) Civilian Labor Force Level - 20 yrs. & over, Black or African American Men	0	0	17	0	0
LNS11000031Q	1972	Q02	4370	nan	10	Q	(Seas) Civilian Labor Force Level - 20 yrs. & over, Black or African American Men	0	0	17	0	0
LNS11000031Q	1972	Q03	4397	nan	10	Q	(Seas) Civilian Labor	0	0	17	0	0

series_id	year	period	value	footnote_codes	fst_code	periodicity_code	series_title	absn_code	activity_code	ages_code	cert_code	c
							Force Level - 20 yrs. & over, Black or African American Men					
LNS11000031Q	1972	Q04	4381	nan	10	Q	(Seas) Civilian Labor Force Level - 20 yrs. & over, Black or African American Men	0	0	17	0	0
LNS11000031Q	1973	Q01	4408	nan	10	Q	(Seas) Civilian Labor Force Level - 20 yrs. & over, Black or African American Men	0	0	17	0	0
LNS11000031Q	1973	Q02	4445	nan	10	Q	(Seas) Civilian Labor Force Level - 20 yrs. & over, Black or African American Men	0	0	17	0	0
LNS11000031Q	1973	Q03	4477	nan	10	Q	(Seas) Civilian Labor Force Level - 20 yrs. & over, Black or African American Men	0	0	17	0	0
LNS11000031Q	1973	Q04	4523	nan	10	Q	(Seas) Civilian Labor Force Level - 20 yrs. & over, Black or African American Men	0	0	17	0	0
LNS11000031Q	1974	Q01	4574	nan	10	Q	(Seas) Civilian Labor Force Level - 20 yrs. & over, Black or African American Men	0	0	17	0	0
LNS11000031Q	1974	Q02	4538	nan	10	Q	(Seas) Civilian Labor Force Level - 20 yrs. & over, Black or African	0	0	17	0	0

series_id	year	period	value	footnote_codes	fst_code	periodicity_code	series_title	absn_code	activity_code	ages_code	cert_code	c
							American					Men

Data access

Azure Notebooks

azureml-opendatasets	<pre>Python # This is a package in preview. from azureml.opendatasets import UsLaborLFS labor = UsLaborLFS() labor_df = labor.to_pandas_dataframe()</pre>
	<pre>Python labor_df.info()</pre>

Azure Databricks

azureml-opendatasets	<pre>Python # This is a package in preview. from azureml.opendatasets import UsLaborLFS labor = UsLaborLFS() labor_df = labor.to_spark_dataframe()</pre>
	<pre>Python display(labor_df.limit(5))</pre>

Azure Synapse

azureml-opendatasets	Sample not available for this platform/package combination.
----------------------	---

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

US Population by County

Article • 12/05/2023

US population by gender and race for each US county sourced from 2000 and 2010 Decennial Census.

This dataset is sourced from United States Census Bureau's [Decennial Census Dataset APIs](#). Review [Terms of Service](#) and [Policies and Notices](#) for the terms and conditions related to the use this dataset.

!**Note**

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Volume and retention

This dataset is stored in Parquet format and has data for the year 2000 and 2010.

Storage location

This dataset is stored in the East US Azure region. Allocating compute resources in East US is recommended for affinity.

Related datasets

- [US Population by ZIP Code](#)

Columns

 [Expand table](#)

Name	Data type	Unique	Values (sample)	Description
countyName	string	1,960	Washington County Jefferson County	County name.
decennialTime	string	2	2010 2000	The time of the decennial census happened, for example, 2010, 2000.
maxAge	int	23	9 66	Max of the age range. If it's null, it's across all ages or the age range has no upper bound, for example, age > 85.
minAge	int	23	35 67	Min of the age range. If it's null, it's across all ages.
population	int	47,229	1 2	Population of this segment.
race	string	8	ASIAN ALONE TWO OR MORE RACES	Race category in Census data. If it's null, it's across all races.
sex	string	3	Male Female	Male or female. If it's null, it's across both sexes.
stateName	string	52	Texas Georgia	Name of the state in US.
year	int	2	2010 2000	Year (in integer) of the decennial time.

Preview

[Expand table](#)

decennialTime	stateName	countyName	population	race	sex	minAge	maxAge	year
2010	Texas	Crockett County	123	WHITE ALONE	Male	5	9	2010
2010	Texas	Crockett County	1	ASIAN ALONE	Female	67	69	2010
2010	Texas	Crockett County	111	WHITE ALONE	Female	55	59	2010
2010	Texas	Crockett County	64	TWO OR MORE RACES	null			2010
2010	Texas	Crockett County	18	null	Male	85		2010
2010	Texas	Crockett County	16	AMERICAN INDIAN AND	Female			2010

decennialTime	stateName	countyName	population	race	sex	minAge	maxAge	year
				ALASKA NATIVE ALONE				
2010	Texas	Crockett County	7	WHITE ALONE	Male	21	21	2010
2010	Texas	Crockett County	45	null	Female	85		2010
2010	Texas	Crockett County	0	NATIVE HAWAIIAN AND OTHER PACIFIC ISLANDER ALONE	Female	67	69	2010

Data access

Azure Notebooks

azureml-opendatasets

Python

```
# This is a package in preview.
from azureml.opendatasets import UsPopulationCounty

population = UsPopulationCounty()
population_df = population.to_pandas_dataframe()
```

Python

```
population_df.info()
```

Azure Databricks

azureml-opendatasets

Python

```
# This is a package in preview.
from azureml.opendatasets import UsPopulationCounty
```

```
population = UsPopulationCounty()
population_df = population.to_spark_dataframe()
```

Python

```
display(population_df.limit(5))
```

Azure Synapse

azureml-opendatasets

Python

```
# This is a package in preview.
from azureml.opendatasets import UsPopulationCounty

population = UsPopulationCounty()
population_df = population.to_spark_dataframe()
```

Python

```
# Display top 5 rows
display(population_df.limit(5))
```

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

US Population by ZIP code

Article • 12/05/2023

US population by gender and race for each US ZIP code sourced from 2000 and 2010 Decennial Census.

This dataset is sourced from United States Census Bureau's [Decennial Census Dataset APIs](#). Review [Terms of Service](#) and [Policies and Notices](#) for the terms and conditions related to the use this dataset.

ⓘ Note

Microsoft provides Azure Open Datasets on an "as is" basis. Microsoft makes no warranties, express or implied, guarantees or conditions with respect to your use of the datasets. To the extent permitted under your local law, Microsoft disclaims all liability for any damages or losses, including direct, consequential, special, indirect, incidental or punitive, resulting from your use of the datasets.

This dataset is provided under the original terms that Microsoft received source data. The dataset may include data sourced from Microsoft.

Volume and retention

This dataset is stored in Parquet format and has data for the year 2010.

Storage location

This dataset is stored in the East US Azure region. Allocating compute resources in East US is recommended for affinity.

Related datasets

- [US Population by County](#)

Columns

[] [Expand table](#)

Name	Data type	Unique	Values (sample)	Description
decennialTime	string	1	2010	The time of the decennial census happened, for example, 2010, 2000.
maxAge	int	23	54 21	Max of the age range. If it's null, it's across all ages or the age range has no upper bound, for example, age > 85.
minAge	int	23	45 30	Min of the age range. If it's null, it's across all ages.
population	int	29,274	1 2	Population of this segment.
race	string	8	SOME OTHER RACE ALONE BLACK OR AFRICAN AMERICAN ALONE	Race category in Census data. If it's null, it's across all races.
sex	string	3	Female Male	Male or female. If it's null, it's across both sexes.
year	int	1	2010	Year (in integer) of the decennial time.
zipCode	string	33,120	39218 87420	5-Digit ZIP Code Tabulation Area (ZCTA5).

Preview

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

decennialTime	zipCode	population	race	sex	minAge	maxAge	year
2010	77477	265	WHITE ALONE	Female	15	17	2010
2010	77477	107	SOME OTHER RACE ALONE	Female	15	17	2010
2010	77477	12	SOME OTHER RACE ALONE	Female	65	66	2010
2010	77477	101	ASIAN ALONE	Female	60	61	2010
2010	77477	221	ASIAN ALONE	Male	10	14	2010

decennialTime	zipCode	population	race	sex	minAge	maxAge	year
2010	77478	256	WHITE ALONE	Female	15	17	2010
2010	77478	17	SOME OTHER RACE ALONE	Female	15	17	2010
2010	77478	3	SOME OTHER RACE ALONE	Female	65	66	2010

Data access

Azure Notebooks

azureml-opendatasets

Python

```
# This is a package in preview.
from azureml.opendatasets import UsPopulationZip

population = UsPopulationZip()
population_df = population.to_pandas_dataframe()
```

Python

```
population_df.info()
```

Azure Databricks

azureml-opendatasets

Python

```
# This is a package in preview.
from azureml.opendatasets import UsPopulationZip

population = UsPopulationZip()
population_df = population.to_spark_dataframe()
```

Python

```
display(population_df.limit(5))
```

Azure Synapse

azureml-opendatasets

Python

```
# This is a package in preview.
from azureml.opendatasets import UsPopulationZip

population = UsPopulationZip()
population_df = population.to_spark_dataframe()
```

Python

```
# Display top 5 rows
display(population_df.limit(5))
```

Next steps

View the rest of the datasets in the [Open Datasets catalog](#).

Azure Government compliance

Article • 04/03/2023

Microsoft Azure Government meets demanding US government compliance requirements that mandate formal assessments and authorizations, including:

- [Federal Risk and Authorization Management Program](#) (FedRAMP)
- Department of Defense (DoD) Cloud Computing [Security Requirements Guide](#) (SRG) Impact Level (IL) 2, 4, and 5

Azure Government maintains the following authorizations that pertain to 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](#) Provisional Authorization (PA) issued by the Defense Information Systems Agency (DISA)
- [DoD IL4](#) PA issued by DISA
- [DoD IL5](#) PA issued by DISA

For links to extra Azure Government compliance assurances, see [Azure compliance](#). For example, Azure Government can help you meet your compliance obligations with many US government requirements, including:

- [Criminal Justice Information Services \(CJIS\)](#)
- [Internal Revenue Service \(IRS\) Publication 1075](#)
- [Defense Federal Acquisition Regulation Supplement \(DFARS\)](#)
- [International Traffic in Arms Regulations \(ITAR\)](#)
- [Export Administration Regulations \(EAR\)](#)
- [Federal Information Processing Standard \(FIPS\) 140](#)
- [National Institute of Standards and Technology \(NIST\) 800-171](#)
- [National Defense Authorization Act \(NDAA\) Section 889 and Section 1634](#)
- [North American Electric Reliability Corporation \(NERC\) Critical Infrastructure Protection \(CIP\) standards](#)
- [Health Insurance Portability and Accountability Act of 1996 \(HIPAA\)](#)
- [Electronic Prescriptions for Controlled Substances \(EPCS\)](#)
- And many more US government, global, and industry standards

For current Azure Government regions and available services, see [Products available by region](#).

Note

- Some Azure services deployed in Azure Government regions (US Gov Arizona, US Gov Texas, and US Gov Virginia) require extra configuration to meet DoD IL5 compute and storage isolation requirements, as explained in [Isolation guidelines for Impact Level 5 workloads](#).
- For DoD IL5 PA compliance scope in Azure Government DoD regions (US DoD Central and US DoD East), see [Azure Government DoD regions IL5 audit scope](#).

Services in audit scope

For a detailed list of Azure, Dynamics 365, Microsoft 365, and Power Platform services in FedRAMP and DoD compliance audit scope, see:

- [Azure public services by audit scope](#)
- [Azure Government services by audit scope](#)

Audit documentation

For information on how to access Azure and Azure Government audit reports and related documentation, see [Azure compliance offerings audit documentation](#).

Azure Policy regulatory compliance built-in initiatives

For extra customer assistance, Microsoft provides Azure Policy regulatory compliance built-in initiatives, which map to **compliance domains** and **controls** in key US government standards, including:

- [FedRAMP High](#)
- [DoD IL4](#)
- [DoD IL5](#)
- And others

For more regulatory compliance built-in initiatives that pertain to Azure Government, see [Azure Policy samples](#).

Regulatory compliance in Azure Policy provides built-in initiative definitions to view a list of the 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 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.

Next steps

- [Azure compliance](#)
- [Azure and other Microsoft services compliance offerings](#)
- [Azure Policy overview](#)
- [Azure Policy regulatory compliance built-in initiatives](#)
- [Azure Government overview](#)
- [Azure Government security](#)
- [Compare Azure Government and global Azure](#)
- [Azure Government services by audit scope](#)
- [Azure Government isolation guidelines for Impact Level 5 workloads](#)
- [Azure Government DoD overview](#)

Azure, Dynamics 365, Microsoft 365, and Power Platform services compliance scope

Article • 11/09/2023

Microsoft Azure cloud environments meet demanding US government compliance requirements that produce formal authorizations, including:

- [Federal Risk and Authorization Management Program](#) (FedRAMP)
- Department of Defense (DoD) Cloud Computing [Security Requirements Guide](#) (SRG) Impact Level (IL) 2, 4, 5, and 6
- [Joint Special Access Program \(SAP\) Implementation Guide \(JSIG\)](#)

Azure (also known as Azure Commercial, Azure Public, or Azure Global) maintains the following authorizations that pertain to all Azure public regions in the United States:

- [FedRAMP High](#) Provisional Authorization to Operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB)
- [DoD IL2](#) Provisional Authorization (PA) issued by the Defense Information Systems Agency (DISA)

Azure Government maintains the following authorizations that pertain to Azure Government regions US Gov Arizona, US Gov Texas, and US Gov Virginia (US Gov regions):

- [FedRAMP High](#) P-ATO issued by the JAB
- [DoD IL2](#) PA issued by DISA
- [DoD IL4](#) PA issued by DISA
- [DoD IL5](#) PA issued by DISA

For current Azure Government regions and available services, see [Products available by region](#).

ⓘ Note

- Some Azure services deployed in Azure Government regions US Gov Arizona, US Gov Texas, and US Gov Virginia (US Gov regions) require extra configuration to meet DoD IL5 compute and storage isolation requirements, as explained in [Isolation guidelines for Impact Level 5 workloads](#).

- For DoD IL5 PA compliance scope in Azure Government regions US DoD Central and US DoD East (US DoD regions), see [US DoD regions IL5 audit scope](#).

Azure Government Secret maintains:

- [DoD IL6](#) PA issued by DISA
- [JSIG PL3](#) ATO (for authorization details, contact your Microsoft account representative)

Azure Government Top Secret maintains:

- [ICD 503](#) ATO with facilities at ICD 705 (for authorization details, contact your Microsoft account representative)
- [JSIG PL3](#) ATO (for authorization details, contact your Microsoft account representative)

This article provides a detailed list of Azure, Dynamics 365, Microsoft 365, and Power Platform cloud services in scope for FedRAMP High, DoD IL2, DoD IL4, DoD IL5, and DoD IL6 authorizations across Azure, Azure Government, and Azure Government Secret cloud environments. For other authorization details in Azure Government Secret and Azure Government Top Secret, contact your Microsoft account representative.

Azure public services by audit scope

Last updated: November 2023

Terminology used

- FedRAMP High = FedRAMP High Provisional Authorization to Operate (P-ATO) in Azure
- DoD IL2 = DoD SRG Impact Level 2 Provisional Authorization (PA) in Azure
-  = service is included in audit scope and has been authorized

 Expand table

Service	FedRAMP High	DoD IL2
Advisor		
AI Builder		

Service	FedRAMP High	DoD IL2
Analysis Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
API Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
App Configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
App Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Application Gateway	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Automation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Entra ID (Free)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Entra ID (P1 + P2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Active Directory B2C	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Entra Domain Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Entra provisioning service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Entra multifactor authentication	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure API for FHIR	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service	FedRAMP High	DoD IL2
Azure Arc-enabled servers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Arc-enabled Kubernetes	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Cache for Redis	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Cosmos DB	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Container Apps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Database for MariaDB	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Database for MySQL	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Database for PostgreSQL	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Databricks **	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure for Education ↗	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Information Protection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Service	FedRAMP High	DoD IL2
Azure Kubernetes Service (AKS)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Marketplace portal ↗	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Maps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Monitor (incl. Application Insights, Log Analytics, and Application Change Analysis)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure NetApp Files	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service	FedRAMP High	DoD IL2
Azure OpenAI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Policy	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Policy's guest configuration	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Red Hat OpenShift	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Resource Manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Service Manager (RDRE)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Sign-up portal ↗	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Sphere	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Spring Apps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Stack Edge (formerly Data Box Edge) *	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Stack HCI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Static WebApps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Video Indexer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Virtual Desktop (formerly Windows Virtual Desktop)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure VMware Solution	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure Web PubSub	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Backup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Bastion	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Service	FedRAMP High	DoD IL2
Batch	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Blueprints	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Bot Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cloud Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cloud Shell	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Cognitive Search (formerly Azure Search)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure AI services: Anomaly Detector	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure AI services: Computer Vision	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure AI services: Content Moderator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure AI services: Containers	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure AI services: Custom Vision	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure AI services: Face	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure AI Language Understanding (LUIS) (part of Azure AI Language)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure AI services: Personalizer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure AI services: QnA Maker (part of Azure AI Language)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service	FedRAMP High	DoD IL2
Azure AI services: Speech	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure AI services: Text Analytics (part of Azure AI Language)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure AI services: Translator	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Container Instances	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Container Registry	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Content Delivery Network (CDN)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Service	FedRAMP High	DoD IL2
Cost Management and Billing	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Customer Lockbox	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data Box *	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data Explorer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data Factory	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Data Share	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Database Migration Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dataverse (incl. Azure Synapse Link for Dataverse)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DDoS Protection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service	FedRAMP High	DoD IL2
Dedicated HSM	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DevTest Labs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
DNS	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dynamics 365 Chat (Omnichannel Engagement Hub)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dynamics 365 Commerce	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dynamics 365 Customer Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dynamics 365 Field Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dynamics 365 Finance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dynamics 365 Fraud Protection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dynamics 365 Guides	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dynamics 365 Sales	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dynamics 365 Sales Professional	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Dynamics 365 Supply Chain Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Event Grid	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Event Hubs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Service	FedRAMP High	DoD IL2
ExpressRoute	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service	FedRAMP High	DoD IL2
File Sync	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Firewall	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Firewall Manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Azure AI Document Intelligence	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Front Door	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Functions	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
GitHub AE ↗	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Health Bot	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HDInsight	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
HPC Cache	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Immersive Reader	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Import/Export	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Internet Analyzer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
IoT Hub	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Key Vault	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service	FedRAMP High	DoD IL2
Lab Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Lighthouse	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Load Balancer	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Logic Apps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Machine Learning	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Managed Applications	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Service	FedRAMP High	DoD IL2
Media Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Metrics Advisor	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Defender XDR (formerly Microsoft Threat Protection)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Azure Attestation	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Azure portal ↗	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Defender for Cloud (formerly Azure Security Center)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Defender for Endpoint (formerly Microsoft Defender Advanced Threat Protection)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Defender for Identity (formerly Azure Advanced Threat Protection)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service	FedRAMP High	DoD IL2
Microsoft Defender for IoT (formerly Azure Security for IoT)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Defender Vulnerability Management	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Graph	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Intune	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Purview (incl. Data Map, Data Estate Insights, and governance portal)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Sentinel (formerly Azure Sentinel)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Stream	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Microsoft Threat Experts	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Migrate	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Network Watcher (incl. Traffic Analytics)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Notification Hubs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Open Datasets	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Peering Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Service	FedRAMP High	DoD IL2
Planned Maintenance for VMs	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power Apps	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power Apps Portal ↗	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service	FedRAMP High	DoD IL2
Power Automate (formerly Microsoft Flow)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power BI	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power BI Embedded	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power Data Integrator for Dataverse (formerly Dynamics 365 Integrator App)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Power Virtual Agents	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Private Link	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Public IP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Resource Graph	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Resource Mover	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Route Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Scheduler (replaced by Logic Apps)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service Bus	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service Fabric	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service Health	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SignalR Service	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service	FedRAMP High	DoD IL2
Site Recovery	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SQL Database	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SQL Managed Instance	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
SQL Server Registry	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Service	FedRAMP High	DoD IL2
SQL Server Stretch Database	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Storage: Archive	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Storage: Blobs (incl. Azure Data Lake Storage Gen2)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Storage: Disks (incl. managed disks)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Storage: Files	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Storage: Queues	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Storage: Tables	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
StorSimple	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Stream Analytics	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Synapse Analytics	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Time Series Insights	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Service	FedRAMP High	DoD IL2
Traffic Manager	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Virtual Machine Scale Sets	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Virtual Machines (incl. Reserved VM Instances)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Virtual Network	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Virtual Network NAT	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Virtual WAN	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VM Image Builder	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
VPN Gateway	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Web Application Firewall	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Windows 10 IoT Core Services	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

* FedRAMP High authorization for edge devices (such as Azure Data Box and Azure Stack Edge) applies only to Azure services that support on-premises, customer-managed devices. For example, FedRAMP High authorization for Azure Data Box covers datacenter infrastructure services and Data Box pod and disk service, which are the

online software components supporting your Data Box hardware appliance. You are wholly responsible for the authorization package that covers the physical devices. For assistance with accelerating your onboarding and authorization of devices, contact your Microsoft account representative.

** FedRAMP High authorization for Azure Databricks is applicable to limited regions in Azure. To configure Azure Databricks for FedRAMP High use, contact your Microsoft or Databricks representative.

Azure Government services by audit scope

Last updated: November 2023

Terminology used

- Azure Government = Azure Government regions US Gov Arizona, US Gov Texas, and US Gov Virginia (US Gov regions)
- FedRAMP High = FedRAMP High Provisional Authorization to Operate (P-ATO) in Azure Government
- DoD IL2 = DoD SRG Impact Level 2 Provisional Authorization (PA) in Azure Government
- DoD IL4 = DoD SRG Impact Level 4 Provisional Authorization (PA) in Azure Government
- DoD IL5 = DoD SRG Impact Level 5 Provisional Authorization (PA) in Azure Government
- DoD IL6 = DoD SRG Impact Level 6 Provisional Authorization (PA) in Azure Government Secret
- = service is included in audit scope and has been authorized

ⓘ Note

- Some services deployed in Azure Government regions US Gov Arizona, US Gov Texas, and US Gov Virginia (US Gov regions) require extra configuration to meet DoD IL5 compute and storage isolation requirements, as explained in [Isolation guidelines for Impact Level 5 workloads](#).
- For DoD IL5 PA compliance scope in Azure Government regions US DoD Central and US DoD East (US DoD regions), see [US DoD regions IL5 audit scope](#).

[Expand table](#)

Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Advisor	✓	✓	✓	✓	✓
AI Builder	✓	✓	✓		
Analysis Services	✓	✓	✓	✓	
API Management	✓	✓	✓	✓	✓
App Configuration	✓	✓	✓	✓	✓
App Service	✓	✓	✓	✓	✓
Application Gateway	✓	✓	✓	✓	✓
Automation	✓	✓	✓	✓	✓
Microsoft Entra ID (Free)	✓	✓	✓	✓	✓
Microsoft Entra ID (P1 + P2)	✓	✓	✓	✓	
Microsoft Entra Domain Services	✓	✓	✓	✓	
Microsoft Entra multifactor authentication	✓	✓	✓	✓	✓
Azure API for FHIR	✓	✓	✓	✓	
Azure Arc-enabled Kubernetes	✓	✓	✓	✓	
Azure Arc-enabled servers	✓	✓	✓	✓	
Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Azure Cache for Redis	✓	✓	✓	✓	✓
Azure Cosmos DB	✓	✓	✓	✓	✓
Azure CXP Nomination Portal	✓	✓	✓	✓	
Azure Database for MariaDB	✓	✓	✓	✓	
Azure Database for MySQL	✓	✓	✓	✓	
Azure Database for PostgreSQL	✓	✓	✓	✓	
Azure Databricks	✓	✓	✓	✓	
Azure Information Protection **	✓	✓	✓	✓	✓

Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Azure Kubernetes Service (AKS)	✓	✓	✓	✓	✓
Azure Maps	✓	✓	✓	✓	✓
Azure Monitor (incl. Application Insights and Log Analytics)	✓	✓	✓	✓	✓
Azure NetApp Files	✓	✓	✓	✓	
Azure Policy	✓	✓	✓	✓	✓
Azure Policy's guest configuration	✓	✓	✓	✓	
Azure Red Hat OpenShift	✓	✓	✓		
Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Azure Resource Manager	✓	✓	✓	✓	✓
Azure Service Manager (RDFF)	✓	✓	✓	✓	✓
Azure Sign-up portal ↗	✓	✓	✓	✓	
Azure Stack Bridge	✓	✓	✓	✓	✓
Azure Stack Edge (formerly Data Box Edge) *	✓	✓	✓	✓	✓
Azure Stack HCI	✓	✓	✓		
Azure Video Indexer	✓	✓	✓		
Azure Virtual Desktop (formerly Windows Virtual Desktop)	✓	✓	✓	✓	✓
Azure VMware Solution	✓	✓			
Backup	✓	✓	✓	✓	✓
Bastion	✓	✓	✓	✓	
Batch	✓	✓	✓	✓	✓
Blueprints	✓	✓	✓	✓	
Bot Service	✓	✓	✓	✓	
Cloud Services	✓	✓	✓	✓	✓
Cloud Shell	✓	✓	✓	✓	✓

Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Cognitive Search (formerly Azure Search)	✓	✓	✓	✓	✓
Azure AI services: Computer Vision	✓	✓	✓	✓	
Azure AI services: Content Moderator	✓	✓	✓	✓	
Azure AI containers	✓	✓	✓	✓	
Azure AI services: Custom Vision	✓	✓	✓	✓	
Azure AI services: Face	✓	✓	✓	✓	
Azure AI services: LUIS (part of Azure AI Language)	✓	✓	✓	✓	✓
Azure AI services: Personalizer	✓	✓	✓	✓	
Azure AI services: QnA Maker (part of Azure AI Language)	✓	✓	✓	✓	
Azure AI Speech	✓	✓	✓	✓	
Azure AI services: Text Analytics (part of Azure AI Language)	✓	✓	✓	✓	
Azure AI services: Translator	✓	✓	✓	✓	
Container Instances	✓	✓	✓	✓	✓
Container Registry	✓	✓	✓	✓	✓
Content Delivery Network (CDN)	✓	✓	✓	✓	✓
Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Cost Management and Billing	✓	✓	✓	✓	
Customer Lockbox	✓	✓	✓	✓	
Data Box *	✓	✓	✓	✓	✓
Data Explorer	✓	✓	✓	✓	✓
Data Factory	✓	✓	✓	✓	✓
Data Share	✓	✓	✓	✓	

Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Database Migration Service	✓	✓	✓	✓	✓
Dataverse (formerly Common Data Service)	✓	✓	✓	✓	✓
DDoS Protection	✓	✓	✓	✓	✓
Dedicated HSM	✓	✓	✓	✓	✓
DevTest Labs	✓	✓	✓	✓	✓
DNS	✓	✓	✓	✓	✓
Dynamics 365 Chat (Omnichannel Engagement Hub)	✓	✓	✓	✓	✓
Dynamics 365 Customer Insights	✓	✓	✓	✓	✓
Dynamics 365 Customer Service	✓	✓	✓	✓	✓
Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Dynamics 365 Customer Voice (formerly Forms Pro)	✓	✓	✓	✓	✓
Dynamics 365 Field Service	✓	✓	✓	✓	✓
Dynamics 365 Finance	✓	✓	✓		
Dynamics 365 Project Service Automation	✓	✓	✓	✓	
Dynamics 365 Sales	✓	✓	✓	✓	
Dynamics 365 Supply Chain Management	✓	✓	✓		
Event Grid	✓	✓	✓	✓	✓
Event Hubs	✓	✓	✓	✓	✓
ExpressRoute	✓	✓	✓	✓	✓
File Sync	✓	✓	✓	✓	
Firewall	✓	✓	✓	✓	✓
Firewall Manager	✓	✓	✓	✓	
Azure AI Document Intelligence	✓	✓	✓	✓	
Front Door	✓	✓	✓	✓	✓

Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Functions	✓	✓	✓	✓	✓
Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
GitHub AE ↗	✓	✓	✓		
HDInsight	✓	✓	✓	✓	✓
HPC Cache	✓	✓	✓	✓	
Import/Export	✓	✓	✓	✓	
IoT Hub	✓	✓	✓	✓	✓
Key Vault	✓	✓	✓	✓	✓
Lab Services	✓	✓	✓	✓	
Lighthouse	✓	✓	✓	✓	
Load Balancer	✓	✓	✓	✓	✓
Logic Apps	✓	✓	✓	✓	✓
Machine Learning	✓	✓	✓	✓	
Managed Applications	✓	✓	✓	✓	
Media Services	✓	✓	✓	✓	✓
Microsoft Defender XDR (formerly Microsoft Threat Protection)	✓	✓	✓	✓	
Microsoft Azure portal	✓	✓	✓	✓	✓
Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Microsoft Azure Government portal	✓	✓	✓	✓	
Microsoft Defender for Cloud (formerly Azure Security Center)	✓	✓	✓	✓	✓
Microsoft Defender for Cloud Apps (formerly Microsoft Cloud App Security)	✓	✓	✓	✓	
Microsoft Defender for Endpoint (formerly Microsoft Defender Advanced Threat Protection)	✓	✓	✓	✓	

Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Microsoft Defender for Identity (formerly Azure Advanced Threat Protection)	✓	✓	✓	✓	✓
Microsoft Defender for IoT (formerly Azure Security for IoT)	✓	✓	✓	✓	✓
Microsoft Defender Vulnerability Management	✓	✓			
Microsoft Graph	✓	✓	✓	✓	✓
Microsoft Intune	✓	✓	✓	✓	✓
Microsoft Purview (incl. Data Map, Data Estate Insights, and governance portal)	✓	✓			
Microsoft Sentinel (formerly Azure Sentinel)	✓	✓	✓	✓	✓
Microsoft Stream	✓	✓	✓	✓	✓
Migrate	✓	✓	✓	✓	✓
Network Watcher (incl. Traffic Analytics)	✓	✓	✓	✓	✓
Notification Hubs	✓	✓	✓	✓	✓
Peering Service	✓	✓	✓	✓	✓
Planned Maintenance for VMs	✓	✓	✓	✓	
Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Power Apps	✓	✓	✓	✓	✓
Power Automate (formerly Microsoft Flow)	✓	✓	✓	✓	✓
Power BI	✓	✓	✓	✓	✓
Power BI Embedded	✓	✓	✓	✓	✓
Power Data Integrator for Dataverse (formerly Dynamics 365 Integrator App)	✓	✓	✓	✓	✓
Power Query Online	✓	✓	✓	✓	✓
Power Virtual Agents	✓	✓	✓		
Private Link	✓	✓	✓	✓	✓
Public IP	✓	✓	✓	✓	

Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Resource Graph	✓	✓	✓	✓	✓
Resource Mover	✓	✓	✓	✓	
Route Server	✓	✓	✓	✓	
Scheduler (replaced by Logic Apps)	✓	✓	✓	✓	
Service Bus	✓	✓	✓	✓	✓
Service Fabric	✓	✓	✓	✓	✓
Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Service Health	✓	✓	✓	✓	
SignalR Service	✓	✓	✓	✓	✓
Site Recovery	✓	✓	✓	✓	
SQL Database	✓	✓	✓	✓	✓
SQL Managed Instance	✓	✓	✓	✓	
SQL Server Stretch Database	✓	✓	✓	✓	
Storage: Archive	✓	✓	✓	✓	
Storage: Blobs (incl. Azure Data Lake Storage Gen2)	✓	✓	✓	✓	✓
Storage: Disks (incl. managed disks)	✓	✓	✓	✓	✓
Storage: Files	✓	✓	✓	✓	
Storage: Queues	✓	✓	✓	✓	✓
Storage: Tables	✓	✓	✓	✓	✓
StorSimple	✓	✓	✓	✓	
Stream Analytics	✓	✓	✓	✓	
Synapse Analytics	✓	✓	✓	✓	✓
Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Synapse Link for Dataverse	✓	✓	✓		

Service	FedRAMP High	DoD IL2	DoD IL4	DoD IL5	DoD IL6
Traffic Manager	✓	✓	✓	✓	✓
Virtual Machine Scale Sets	✓	✓	✓	✓	✓
Virtual Machines (incl. Reserved VM Instances)	✓	✓	✓	✓	✓
Virtual Network	✓	✓	✓	✓	✓
Virtual Network NAT	✓	✓	✓	✓	
Virtual WAN	✓	✓	✓	✓	✓
VM Image Builder	✓	✓	✓		
VPN Gateway	✓	✓	✓	✓	✓
Web Application Firewall	✓	✓	✓	✓	

* Authorizations for edge devices (such as Azure Data Box and Azure Stack Edge) apply only to Azure services that support on-premises, customer-managed devices. You are wholly responsible for the authorization package that covers the physical devices. For assistance with accelerating your onboarding and authorization of devices, contact your Microsoft account representative.

** Azure Information Protection (AIP) is part of the Microsoft Purview Information Protection solution - it extends the labeling and classification functionality provided by Microsoft 365. Before AIP can be used for DoD workloads at a given impact level (IL), the corresponding Microsoft 365 services must be authorized at the same IL.

Next steps

- [Acquiring and accessing Azure Government ↗](#)
- [Azure Government overview](#)
- [Azure Government security](#)
- [FedRAMP High](#)
- [DoD Impact Level 2](#)
- [DoD Impact Level 4](#)
- [DoD Impact Level 5](#)
- [DoD Impact Level 6](#)
- [Azure Government isolation guidelines for Impact Level 5 workloads](#)
- [Azure guidance for secure isolation](#)

Details of the Microsoft cloud security benchmark (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 Microsoft cloud security benchmark (Azure Government). For more information about this compliance standard, see [Microsoft cloud security benchmark](#). To understand *Ownership*, see [Azure Policy policy definition](#) and [Shared responsibility in the cloud](#).

The following mappings are to the **Microsoft cloud security benchmark** 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 **Microsoft cloud security benchmark** 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](#) ↗.

Network Security

Establish network segmentation boundaries

ID: Microsoft cloud security benchmark NS-1 **Ownership:** Shared

ⓘ [Expand table](#)

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 ↗
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 https://aka.ms/nsg-doc ↗	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 https://aka.ms/nsg-doc ↗	AuditIfNotExists, Disabled	3.0.0 ↗
Subnets should be associated with a Network Security Group ↗	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 ↗

Secure cloud services with network controls

ID: Microsoft cloud security benchmark NS-2 Ownership: Shared

Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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	Azure Private Link lets you connect your virtual network to Azure services without a public IP address at the source or	AuditIfNotExists, Disabled	1.0.2 ↗

Name should use private link ↗ (Azure portal)	Description 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: https://aka.ms/appconfig/private-endpoint .	Effect(s)	Version (GitHub)
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	2.0.0 ↗
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: https://docs.microsoft.com/azure/azure-cache-for-redis/cache-private-link .	AuditIfNotExists, Disabled	1.0.0 ↗
Azure Cosmos DB accounts should have firewall rules ↗	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.	Audit, Deny, Disabled	2.0.0 ↗
Azure Cosmos DB should disable public network access ↗	Disabling public network access improves security by ensuring that your CosmosDB account isn't exposed on the public internet. Creating private endpoints can limit exposure of your CosmosDB account. Learn more at: https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints#blocking-public-network-access-during-account-creation .	Audit, Deny, Disabled	1.0.0 ↗
Azure Databricks Clusters should disable public IP ↗	Disabling public IP of clusters in Azure Databricks Workspaces improves security by ensuring that the clusters aren't exposed on the public internet. Learn more at: https://learn.microsoft.com/azure/databricks/security/secure-cluster-connectivity .	Audit, Deny, Disabled	1.0.1 ↗
Azure Databricks Workspaces should be in a virtual network ↗	Azure Virtual Networks provide enhanced security and isolation for your Azure Databricks Workspaces, as well as subnets, access control policies, and other features to further restrict access. Learn more at: https://docs.microsoft.com/azure/databricks/administration-guide/cloud-configurations/azure/vnet-inject .	Audit, Deny, Disabled	1.0.2 ↗
Azure Databricks	Disabling public network access improves security by ensuring that the resource isn't exposed on the public	Audit, Deny, Disabled	1.0.1 ↗

Name	Description	Effect(s)	Version
(Azure portal)	(GitHub)		
Workspaces should disable public network access ↗	internet. You can control exposure of your resources by creating private endpoints instead. Learn more at: https://learn.microsoft.com/azure/databricks/administration-guide/cloud-configurations/azure/private-link .		
Azure Databricks Workspaces 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 Azure Databricks workspaces, you can reduce data leakage risks. Learn more about private links at: https://aka.ms/adbpe .	Audit, Disabled	1.0.2 ↗
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: https://aka.ms/privateendpoints .	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: https://aka.ms/privateendpoints .	Audit, Disabled	1.0.2 ↗
Azure Machine Learning Computes should be in a virtual network ↗	Azure Virtual Networks provide enhanced security and isolation for your Azure Machine Learning Compute Clusters and Instances, as well as subnets, access control policies, and other features to further restrict access. When a compute is configured with a virtual network, it is not publicly addressable and can only be accessed from virtual machines and applications within the virtual network.	Audit, Disabled	1.0.1 ↗
Azure Machine Learning Workspaces should disable public network access ↗	Disabling public network access improves security by ensuring that the Machine Learning Workspaces aren't exposed on the public internet. You can control exposure of your workspaces by creating private endpoints instead. Learn more at: https://learn.microsoft.com/azure/machine-	Audit, Deny, Disabled	2.0.1 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
public network access ↗	learning/how-to-configure-private-link?view=azureml-api-2&tabs=azure-portal.		
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: https://docs.microsoft.com/azure/machine-learning/how-to-configure-private-link .	Audit, 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: https://aka.ms/asrs/privatelink .	Audit, Disabled	1.0.0 ↗
Azure SQL Managed Instances should disable public network access ↗	Disabling public network access (public endpoint) on Azure SQL Managed Instances improves security by ensuring that they can only be accessed from inside their virtual networks or via Private Endpoints. To learn more about public network access, visit https://aka.ms/mi-public-endpoint .	Audit, Deny, 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 https://go.microsoft.com/fwlink/?linkid=2129800 . 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 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 ↗

Name	Description	Effect(s)	Version
(Azure portal)	(GitHub)		
network access ↗	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: https://go.microsoft.com/fwlink/?linkid=2129800 .	Audit, Disabled	3.0.0 ↗
Container registries should not allow unrestricted network access ↗	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: https://aka.ms/acr/privatelink , https://aka.ms/acr/portal/public-network and https://aka.ms/acr/vnet .	Audit, Deny, Disabled	2.0.0 ↗
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: https://aka.ms/acr/private-link .	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: https://docs.microsoft.com/azure/cosmos-db/how-to-configure-private-endpoints .	Audit, Disabled	1.0.0 ↗
Private endpoint connections on Azure SQL Database	Private endpoint connections enforce secure communication by enabling private connectivity to Azure SQL Database.	Audit, Disabled	1.1.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
should be enabled ↗			
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 ↗
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 using virtual network rules ↗	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 ↗
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 - https://aka.ms/azureprivatelinkoverview ↗	AuditIfNotExists, Disabled	2.0.0 ↗

Deploy firewall at the edge of enterprise network

ID: Microsoft cloud security benchmark NS-3 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 ↗
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 ↗
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 ↗

Deploy DDOS protection

ID: Microsoft cloud security benchmark NS-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 ↗

Deploy web application firewall

ID: Microsoft cloud security benchmark NS-6 Ownership: Shared

 Expand table

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 ↗
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 ↗

Detect and disable insecure services and protocols

ID: Microsoft cloud security benchmark NS-8 Ownership: Shared

 Expand table

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

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
latest TLS version ↴	latest TLS version for Function apps to take advantage of security fixes, if any, and/or new functionalities of the latest version.		

Ensure Domain Name System (DNS) security

ID: Microsoft cloud security benchmark NS-10 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
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 https://aka.ms/defender-for-dns . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: https://aka.ms/pricing-security-center ↴	AuditIfNotExists, Disabled	1.0.0 ↴

Identity Management

Use centralized identity and authentication system

ID: Microsoft cloud security benchmark IM-1 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(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	AuditIfNotExists, Disabled	1.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	management of database users and other Microsoft services		
Azure Machine Learning Computes should have local authentication methods disabled ↗	Disabling local authentication methods improves security by ensuring that Machine Learning Computes require Azure Active Directory identities exclusively for authentication. Learn more at: https://aka.ms/azure-ml-aad-policy ↗ .	Audit, Deny, Disabled	2.0.1 ↗
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: https://aka.ms/cs/auth ↗ .	Audit, Deny, Disabled	1.0.0 ↗
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 ↗
Storage accounts should prevent shared key access ↗	Audit requirement of Azure Active Directory (Azure AD) to authorize requests for your storage account. By default, requests can be authorized with either Azure Active Directory credentials, or by using the account access key for Shared Key authorization. Of these two types of authorization, Azure AD provides superior security and ease of use over Shared Key, and is recommended by Microsoft.	Audit, Deny, Disabled	2.0.0 ↗
VPN gateways should use only Azure Active Directory (Azure AD) authentication for point-to-site users ↗	Disabling local authentication methods improves security by ensuring that VPN Gateways use only Azure Active Directory identities for authentication. Learn more about Azure AD authentication at https://docs.microsoft.com/azure/vpn-gateway/openvpn-azure-ad-tenant	Audit, Deny, Disabled	1.0.0 ↗

Manage application identities securely and automatically

ID: Microsoft cloud security benchmark IM-3 **Ownership:** Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
App Service apps should use managed identity ↗	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	3.0.0 ↗
Function apps should use managed identity ↗	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	3.0.0 ↗
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 https://aka.ms/gcpol ↗	AuditIfNotExists, Disabled	1.0.1 ↗

Authenticate server and services

ID: Microsoft cloud security benchmark IM-4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure SQL Database should be running TLS version 1.2 or newer ↗	Setting TLS version to 1.2 or newer improves security by ensuring your Azure SQL Database can only be accessed from clients using TLS 1.2 or newer. Using versions of TLS less than 1.2 is not recommended since they have well documented security vulnerabilities.	Audit, Disabled, Deny	2.0.0 ↗

Use strong authentication controls

ID: Microsoft cloud security benchmark IM-6 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 ↗

Privileged Access

Separate and limit highly privileged/administrative users

ID: Microsoft cloud security benchmark PA-1 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 ↗
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 ↗
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 ↗
There should be more than one owner assigned	It is recommended to designate more than one subscription owner in order	AuditIfNotExists, Disabled	3.0.0 ↗

Name	Description	Effect(s)	Version
To your subscription ↗ (Azure portal)	Do have administrator access redundancy.		(GitHub)

Avoid standing access for accounts and permissions

ID: Microsoft cloud security benchmark PA-2 **Ownership: Shared**

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

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

Review and reconcile user access regularly

ID: Microsoft cloud security benchmark PA-4 **Ownership: Shared**

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

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

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	1.0.0 ↗

Follow just enough administration (least privilege) principle

ID: Microsoft cloud security benchmark PA-7 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Azure Role-Based Access Control (RBAC) should be used on Kubernetes Services ↗	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	1.0.3 ↗

Data Protection

Monitor anomalies and threats targeting sensitive data

ID: Microsoft cloud security benchmark DP-2 Ownership: Shared

[Expand table](#)

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	AuditIfNotExists, Disabled	1.0.2 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Defender for SQL should be enabled for unprotected SQL Managed Instances ↗	threats to SQL databases, and discovering and classifying sensitive data.	AuditIfNotExists, Disabled	1.0.2 ↗
Microsoft Defender for Storage (Classic) should be enabled ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.4 ↗
Microsoft Defender for Storage (Classic) provides detections of unusual and potentially harmful attempts to access or exploit storage accounts. ↗	Microsoft Defender for Storage (Classic) provides detections of unusual and potentially harmful attempts to access or exploit storage accounts.	AuditIfNotExists, Disabled	1.0.4 ↗

Encrypt sensitive data in transit

ID: Microsoft cloud security benchmark DP-3 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 SQL Database should be running TLS version 1.2 or newer ↗	Setting TLS version to 1.2 or newer improves security by ensuring your Azure SQL Database can only be accessed from clients using TLS 1.2 or newer. Using versions of TLS less than 1.2 is not recommended since they have well documented security vulnerabilities.	Audit, Disabled, Deny	2.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Enforce SSL connection should be enabled for MySQL database servers ↗	<p>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.</p>	Audit, Disabled	1.0.1 ↗
Enforce SSL connection should be enabled for PostgreSQL database servers ↗	<p>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.</p>	Audit, Disabled	1.0.1 ↗
Function apps should only be accessible over HTTPS ↗	<p>Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks.</p>	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 ↗	<p>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.</p>	AuditIfNotExists, Disabled	2.0.1 ↗
Kubernetes clusters should be accessible only over HTTPS ↗	<p>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 https://aka.ms/kubepolicydoc ↗</p>	audit, Audit, deny, Deny, disabled, Disabled	9.1.0 ↗
Only secure connections to your Azure Cache for	<p>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</p>	Audit, Deny, Disabled	1.0.0 ↗

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Redis should be enabled ↴	layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking		
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 ↴

Enable data at rest encryption by default

ID: Microsoft cloud security benchmark DP-4 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Automation account variables should be encrypted ↴	It is important to enable encryption of Automation account variable assets when storing sensitive data	Audit, Deny, 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 ↴
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 and virtual machine scale sets should have encryption at host enabled ↴	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	Audit, Deny, Disabled	1.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	customer-managed or platform-managed key, depending on the encryption type selected on the disk. Learn more at https://aka.ms/vm-hbe .		
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: https://aka.ms/disksse , ↗ Different disk encryption offerings: https://aka.ms/diskencryptioncomparison ↗	AuditIfNotExists, Disabled	2.0.3 ↗

Use customer-managed key option in data at rest encryption when required

ID: Microsoft cloud security benchmark DP-5 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Azure Cosmos DB accounts should use customer-managed keys to encrypt data at rest ↗	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, including rotation and management. Learn more at https://aka.ms/cosmosdb-cmk .	audit, Audit, deny, Deny, disabled, Disabled	1.1.0 ↗
Azure Machine Learning workspaces should be encrypted with 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	Audit, Deny, Disabled	1.0.3 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
customer-managed key ↗	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 https://aka.ms/azureml-workspaces-cmk ↗.		
Cognitive Services accounts should enable data encryption with a customer-managed key ↗	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 https://go.microsoft.com/fwlink/?linkid=2121321 ↗.	Audit, Deny, Disabled	2.1.0 ↗
Container registries should be encrypted with a customer-managed key ↗	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 https://aka.ms/acr/CMK ↗.	Audit, Deny, Disabled	1.1.2 ↗
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 ↗

Ensure security of key and certificate repository

ID: Microsoft cloud security benchmark DP-8 Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Key vaults should have deletion protection enabled ↗	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	2.1.0 ↗
Key vaults should have soft delete enabled ↗	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	3.0.0 ↗
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	5.0.0 ↗

Asset Management

Use only approved services

ID: Microsoft cloud security benchmark AM-2 Ownership: Shared

Expand table

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

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

Use only approved applications in virtual machine

ID: Microsoft cloud security benchmark AM-5 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	3.0.0 ↴
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	3.0.0 ↴

Logging and Threat Detection

Enable threat detection capabilities

Name	Description	Effect(s)	Version
(Azure portal)			(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 https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc .	AuditIfNotExists, Disabled	4.0.1- preview ↗
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 https://aka.ms/defender-for-dns ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: https://aka.ms/pricing-security-center ↗ .	AuditIfNotExists, Disabled	1.0.0 ↗
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 https://aka.ms/defender-for-resource-manager ↗ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: https://aka.ms/pricing-security-center ↗ .	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 should be enabled for unprotected SQL Managed Instances ↗	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↗
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 (Classic) should be enabled ↗	Microsoft Defender for Storage (Classic) provides detections of unusual and potentially harmful attempts to access or exploit storage accounts.	AuditIfNotExists, Disabled	1.0.4 ↗

Enable threat detection for identity and access management

ID: Microsoft cloud security benchmark LT-2 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 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	AuditIfNotExists, Disabled	4.0.1-preview ↗

Name	Description	Effect(s)	Version
(Azure portal)	(GitHub)		
Microsoft Defender for Cloud extension installed ↳	more in https://docs.microsoft.com/azure/defender-for-cloud/defender-for-containers-enable?pivots=defender-for-container-arc .		
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 https://aka.ms/defender-for-dns . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0 ↳
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 https://aka.ms/defender-for-resource-manager . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: https://aka.ms/pricing-security-center .	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 should be enabled	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↳

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
for unprotected SQL Managed Instances ↗			
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 (Classic) should be enabled ↗	Microsoft Defender for Storage (Classic) provides detections of unusual and potentially harmful attempts to access or exploit storage accounts.	AuditIfNotExists, Disabled	1.0.4 ↗

Enable logging for security investigation

ID: Microsoft cloud security benchmark LT-3 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
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)
Resource logs in Azure Databricks Workspaces should be enabled ↗	Resource logs enable recreating activity trails to use for investigation purposes when a security incident occurs or when your network is compromised.	AuditIfNotExists, Disabled	1.0.1 ↗
Resource logs in Azure Kubernetes Service should be enabled ↗	Azure Kubernetes Service's resource logs can help recreate activity trails when investigating security incidents. Enable it to make sure the logs will exist when needed	AuditIfNotExists, Disabled	1.0.0 ↗
Resource logs in Azure Machine Learning Workspaces should be enabled ↗	Resource logs enable recreating activity trails to use for investigation purposes when a security incident occurs or when your network is compromised.	AuditIfNotExists, Disabled	1.0.1 ↗
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	5.0.0 ↗
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	5.0.0 ↗
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	5.0.0 ↗
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	5.0.0 ↗
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	5.0.0 ↗
Resource logs in Logic Apps should be enabled ↗	Audit enabling of resource logs. This enables you to recreate activity trails to	AuditIfNotExists, Disabled	5.1.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
enabled ↗	use for investigation purposes; when a security incident occurs or when your network is compromised		
Resource logs in Search services 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 ↗
Resource logs in Service Bus 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 ↗

Centralize security log management and analysis

ID: Microsoft cloud security benchmark LT-5 Ownership: Shared

[Expand table](#)

Name (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 ↗
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	1.0.0 ↗

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

Configure log storage retention

ID: Microsoft cloud security benchmark LT-6 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
SQL servers with auditing to storage account destination should be configured with 90 days retention or higher ↴	For incident investigation purposes, we recommend setting the data retention for your SQL Server' auditing to storage account destination to at least 90 days. 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.	AuditIfNotExists, Disabled	3.0.0 ↴

Incident Response

Preparation - setup incident notification

ID: Microsoft cloud security benchmark IR-2 Ownership: Shared

[Expand table](#)

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

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

Detection and analysis - create incidents based on high-quality alerts

ID: Microsoft cloud security benchmark IR-3 Ownership: Shared

 Expand table

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 https://aka.ms/defender-for-dns ↴ . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: https://aka.ms/pricing-security-center ↴ .	AuditIfNotExists, Disabled	1.0.0 ↴
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 about suspicious	AuditIfNotExists, Disabled	1.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
should be enabled ↴	activity. Learn more about the capabilities of Azure Defender for Resource Manager at https://aka.ms/defender-for-resource-manager . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: https://aka.ms/pricing-security-center .		
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 should be enabled for unprotected SQL Managed Instances ↴	Audit each SQL Managed Instance without advanced data security.	AuditIfNotExists, Disabled	1.0.2 ↴
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 (Classic) should be enabled ↴	Microsoft Defender for Storage (Classic) provides detections of unusual and potentially harmful attempts to access or exploit storage accounts.	AuditIfNotExists, Disabled	1.0.4 ↴

Detection and analysis - investigate an incident

ID: Microsoft cloud security benchmark IR-4 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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	AuditIfNotExists, Disabled	3.0.0 ↴

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

Detection and analysis - prioritize incidents

ID: AMicrosoft cloud security benchmark IR-5 Ownership: Shared

Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(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 https://aka.ms/defender-for-dns . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0
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 https://aka.ms/defender-for-resource-manager . Enabling this Azure Defender plan results in charges. Learn about the pricing details per region on Security Center's pricing page: https://aka.ms/pricing-security-center .	AuditIfNotExists, Disabled	1.0.0
Azure Defender for servers	Azure Defender for servers provides real-time threat protection for server workloads and	AuditIfNotExists, Disabled	1.0.3

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
should be enabled ↴	generates hardening recommendations as well as alerts about suspicious activities.		
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 ↴
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 (Classic) should be enabled ↴	Microsoft Defender for Storage (Classic) provides detections of unusual and potentially harmful attempts to access or exploit storage accounts.	AuditIfNotExists, Disabled	1.0.4 ↴

Posture and Vulnerability Management

Audit and enforce secure configurations

ID: Microsoft cloud security benchmark PV-2 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
[Deprecated]: Function apps should have 'Client Certificates (Incoming client certificates)' enabled ↴	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	3.1.0-deprecated ↴
App Service apps should have Client Certificates	Client certificates allow for the app to request a certificate for incoming requests. Only clients that have a	AuditIfNotExists, Disabled	1.0.0 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
(Incoming client certificates) enabled	valid certificate will be able to reach the app. This policy applies to apps with Http version set to 1.1.		
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
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
Azure Machine Learning compute instances should be recreated to get the latest software updates	Ensure Azure Machine Learning compute instances run on the latest available operating system. Security is improved and vulnerabilities reduced by running with the latest security patches. For more information, visit https://aka.ms/azureml-ci-updates .	[parameters('effects')]	1.0.3
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
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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 https://aka.ms/kubepolicydoc ↗.	audit, Audit, deny, Deny, disabled, Disabled	10.1.0 ↗
Kubernetes cluster containers should not share host process ID or host IPC namespace ↗	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 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 https://aka.ms/kubepolicydoc ↗.	audit, Audit, deny, Deny, disabled, Disabled	6.1.0 ↗
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 https://aka.ms/kubepolicydoc ↗.	audit, Audit, deny, Deny, disabled, Disabled	7.1.1 ↗
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 https://aka.ms/kubepolicydoc ↗.	audit, Audit, deny, Deny, disabled, Disabled	7.1.0 ↗
Kubernetes cluster containers	Use images from trusted registries to reduce the Kubernetes cluster's exposure risk to unknown	audit, Audit, deny, Deny, disabled, Disabled	10.1.1 ↗

Name only use allowed images <small>(Azure portal)</small>	Description This policy, security issues and malicious images. For more information, see https://aka.ms/kubepolicydoc .	Effect(s)	Version (GitHub)
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 run-time 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 https://aka.ms/kubepolicydoc .	audit, Audit, deny, Deny, disabled, Disabled	7.1.0
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 https://aka.ms/kubepolicydoc .	audit, Audit, deny, Deny, disabled, Disabled	7.1.1
Kubernetes cluster pods and containers should only run with approved user and group IDs	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 https://aka.ms/kubepolicydoc .	audit, Audit, deny, Deny, disabled, Disabled	7.1.1
Kubernetes cluster pods should only use approved host network and port range	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 https://aka.ms/kubepolicydoc .	audit, Audit, deny, Deny, disabled, Disabled	7.1.0
Kubernetes cluster services	Restrict services to listen only on allowed ports to secure access to the Kubernetes cluster. This policy is	audit, Audit, deny, Deny, disabled, Disabled	9.1.0

Name Should listen only on allowed ports (Azure portal)	Description Available for Kubernetes Service (AKS), and preview for Azure Arc enabled Kubernetes. For more information, see https://aka.ms/kubepolicydoc .	Effect(s)	Version (GitHub)
Kubernetes cluster should not allow privileged containers	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 https://aka.ms/kubepolicydoc .	audit, Audit, deny, Deny, disabled, Disabled	10.1.0
Kubernetes clusters should disable automounting API credentials	Disable automounting API credentials to prevent a potentially compromised Pod resource to run API commands against Kubernetes clusters. For more information, see https://aka.ms/kubepolicydoc .	audit, Audit, deny, Deny, disabled, Disabled	5.1.0
Kubernetes clusters should not allow container privilege escalation	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 information, see https://aka.ms/kubepolicydoc .	audit, Audit, deny, Deny, disabled, Disabled	8.1.0
Kubernetes clusters should not grant CAP_SYS_ADMIN security capabilities	To reduce the attack surface of your containers, restrict CAP_SYS_ADMIN Linux capabilities. For more information, see https://aka.ms/kubepolicydoc .	audit, Audit, deny, Deny, disabled, Disabled	6.1.0
Kubernetes clusters should not use the default namespace	Prevent usage of the default namespace in Kubernetes clusters to protect against unauthorized access for ConfigMap, Pod, Secret, Service, and ServiceAccount resource types.	audit, Audit, deny, Deny, disabled, Disabled	5.1.0

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
For more information, see https://aka.ms/kubepolicydoc .			

Audit and enforce secure configurations for compute resources

ID: Microsoft cloud security benchmark PV-4 Ownership: Shared

 Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
[Preview]: Guest Attestation extension should be installed on supported Linux virtual machines	Install Guest Attestation extension on supported Linux virtual machines to allow Azure Security Center to proactively attest and monitor the boot integrity. Once installed, boot integrity will be attested via Remote Attestation. This assessment applies to Trusted Launch and Confidential Linux virtual machines.	AuditIfNotExists, Disabled	6.0.0-preview
[Preview]: Guest Attestation extension should be installed on supported Linux virtual machines scale sets	Install Guest Attestation extension on supported Linux virtual machines scale sets to allow Azure Security Center to proactively attest and monitor the boot integrity. Once installed, boot integrity will be attested via Remote Attestation. This assessment applies to Trusted Launch and Confidential Linux virtual machine scale sets.	AuditIfNotExists, Disabled	5.1.0-preview
[Preview]: Guest Attestation extension should be installed on supported Windows virtual machines	Install Guest Attestation extension on supported virtual machines to allow Azure Security Center to proactively attest and monitor the boot integrity. Once installed, boot integrity will be attested via Remote Attestation. This assessment applies to Trusted Launch and Confidential Windows virtual machines.	AuditIfNotExists, Disabled	4.0.0-preview
[Preview]: Guest Attestation extension should be installed on supported Windows virtual machine scale sets	Install Guest Attestation extension on supported virtual machines scale sets to allow Azure Security Center to proactively attest and monitor the boot integrity. Once installed, boot integrity will be attested via Remote Attestation. This assessment applies to Trusted Launch and Confidential Windows virtual machine scale sets.	AuditIfNotExists, Disabled	3.1.0-preview

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
machines scale sets ↗	to Trusted Launch and Confidential Windows virtual machine scale sets.		
[Preview]: Secure Boot should be enabled on supported Windows virtual machines ↗	Enable Secure Boot on supported Windows virtual machines to mitigate against malicious and unauthorized changes to the boot chain. Once enabled, only trusted bootloaders, kernel and kernel drivers will be allowed to run. This assessment applies to Trusted Launch and Confidential Windows virtual machines.	Audit, Disabled	4.0.0-preview ↗
[Preview]: vTPM should be enabled on supported virtual machines ↗	Enable virtual TPM device on supported virtual machines to facilitate Measured Boot and other OS security features that require a TPM. Once enabled, vTPM can be used to attest boot integrity. This assessment only applies to trusted launch enabled virtual machines.	Audit, Disabled	2.0.0-preview ↗
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 https://aka.ms/gcpol ↗ .	AuditIfNotExists, Disabled	1.0.2 ↗
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 https://aka.ms/gcpol ↗	AuditIfNotExists, Disabled	1.0.1 ↗

Rapidly and automatically remediate vulnerabilities

ID: Microsoft cloud security benchmark PV-6 Ownership: Shared

 Expand table

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Container registry images should have vulnerability findings resolved (powered by Microsoft Defender Vulnerability Management) ↗	Container image vulnerability assessment scans your registry for commonly known vulnerabilities (CVEs) and provides a detailed vulnerability report for each image. Resolving vulnerabilities can greatly improve your security posture, ensuring images are safe to use prior to deployment.	AuditIfNotExists, Disabled	1.0.0 ↗
Running container images should have vulnerability findings resolved (powered by Microsoft Defender Vulnerability Management) ↗	Container image vulnerability assessment scans your registry for commonly known vulnerabilities (CVEs) and provides a detailed vulnerability report for each image. This recommendation provides visibility to vulnerable images currently running in your Kubernetes clusters. Remediating vulnerabilities in container images that are currently running is key to improving your security posture, significantly reducing the attack surface for your containerized workloads.	AuditIfNotExists, Disabled	1.0.0 ↗
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 ↗
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	3.0.0 ↗

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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	3.0.0 ↗
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 ↗
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	3.0.0 ↗

Endpoint Security

Use Endpoint Detection and Response (EDR)

ID: Microsoft cloud security benchmark ES-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 ↗

Use modern anti-malware software

ID: Microsoft cloud security benchmark ES-2 Ownership: Shared

↔ [Expand table](#)

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	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	3.1.0 ↗

Backup and Recovery

Ensure regular automated backups

ID: Microsoft cloud security benchmark BR-1 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 ↗
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	Audit, Disabled	1.0.1 ↗

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.			
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	1.0.1 ↴

Protect backup and recovery data

ID: Microsoft cloud security benchmark BR-2 Ownership: Shared

[Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Ensure protection of your Azure Virtual Machines by enabling Azure Backup. Azure Backup is a secure and cost effective data protection solution for Azure.			
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	3.0.0 ↴
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	Audit, Disabled	1.0.1 ↴

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
	paired region to provide recovery option in case of a region failure. Configuring geo-redundant storage for backup is only allowed during server create.		
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	1.0.1 ↗

DevOps Security

Enforce security of workload throughout DevOps lifecycle

ID: Microsoft cloud security benchmark DS-6 Ownership: Shared

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Container registry images should have vulnerability findings resolved (powered by Microsoft Defender Vulnerability Management) ↗	Container image vulnerability assessment scans your registry for commonly known vulnerabilities (CVEs) and provides a detailed vulnerability report for each image. Resolving vulnerabilities can greatly improve your security posture, ensuring images are safe to use prior to deployment.	AuditIfNotExists, Disabled	1.0.0 ↗
Running container images should have	Container image vulnerability assessment scans your registry for commonly known	AuditIfNotExists, Disabled	1.0.0 ↗

Name	Description	Effect(s)	Version (GitHub)
Vulnerabilities resolved (powered by Azure portal) Microsoft Defender Vulnerability Management	Vulnerabilities (CVEs) and provides a detailed vulnerability report for each image. This recommendation provides visibility to vulnerable images currently running in your Kubernetes clusters. Remediating vulnerabilities in container images that are currently running is key to improving your security posture, significantly reducing the attack surface for your containerized workloads.		
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

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](#).

Azure support for export controls

Article • 05/31/2023

To help you navigate export control rules, Microsoft has published the [Microsoft Azure Export Controls](#) whitepaper. It describes US export controls particularly as they apply to software and technical data, reviews potential sources of export control risks, and offers specific guidance to help you assess your obligations under these controls. Extra information is available from the Cloud Export FAQ, which is accessible from Frequently Asked Questions on [Exporting Microsoft products](#).

ⓘ Note

Disclaimer: You're wholly responsible for ensuring your own compliance with all applicable laws and regulations. Information provided in this article doesn't constitute legal advice, and you should consult your legal advisor for any questions regarding regulatory compliance.

Overview of export control laws

Export related definitions vary somewhat among various export control regulations. In simplified terms, an export often implies a transfer of restricted information, materials, equipment, software, and so on, to a foreign person or foreign destination by any means. US export control policy is enforced through export control laws and regulations administered primarily by the Department of Commerce, Department of State, Department of Energy, Nuclear Regulatory Commission, and Department of Treasury. Respective agencies within each department are responsible for specific areas of export control based on their historical administration, as shown in Table 1.

Table 1. US export control laws and regulations

Regulator	Law/Regulation	Reference
Department of Commerce: Bureau of Industry and Security (BIS)	- Export Administration Act (EAA) of 1979 - Export Administration Regulations (EAR)	- P.L. 96-72 - 15 CFR Parts 730 – 774
Department of State: Directorate of Defense Trade Controls (DDTC)	- Arms Export Control Act (AECA) - International Traffic in Arms Regulations (ITAR)	- 22 U.S.C. 39 - 22 CFR Parts 120 – 130

Regulator	Law/Regulation	Reference
Department of Energy: National Nuclear Security Administration (NNSA)	- Atomic Energy Act of 1954 (AEA) - Assistance to Foreign Atomic Energy Activities	- 42 U.S.C. 2011 et. seq. - 10 CFR Part 810
Nuclear Regulatory Commission (NRC)	- Nuclear Non-Proliferation Act of 1978 - Export and Import of Nuclear Equipment and Materials	- P.L. 95-242 - 10 CFR Part 110
Department of Treasury: Office of Foreign Assets Control (OFAC)	- Trading with the Enemy Act (TWEA) - Foreign Assets Control Regulations	- 50 U.S.C. Sections 5 and 16 - 31 CFR Part 500

This article contains a review of the current US export control regulations, considerations for cloud computing, and Azure features and commitments in support of export control requirements.

EAR

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 Federal Information Processing Standard (FIPS) 140 validated cryptographic modules and not intentionally stored in a military-embargoed country/region, that is, Country/Region 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.

Both Azure and Azure Government can help you meet your EAR compliance requirements. Except for the Azure region in Hong Kong SAR, Azure and Azure Government datacenters aren't located in proscribed countries/regions 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 extra assurances, see [How does Azure Key Vault protect your keys?](#)

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

Azure Government provides an extra layer of protection through contractual commitments regarding storage of your customer data in the United States and limiting potential access to systems processing your data to [screened US persons](#). For more information about Azure support for EAR, see [Azure EAR compliance offering](#).

ITAR

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 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/region proscribed in § 126.1](#) or the Russian Federation, and 5) not sent from a country/region 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 always kept encrypted between the originator and intended recipient, and the means of decryption isn't provided to any third party.

There's no ITAR compliance certification; however, both Azure and Azure Government can help you meet your ITAR compliance obligations. Except for the Azure region in Hong Kong SAR, Azure and Azure Government datacenters aren't located in proscribed countries/regions 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 extra assurances, see [How does Azure Key Vault protect your keys?](#)

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

Azure Government provides an extra layer of protection through contractual commitments regarding storage of your customer data in the United States and limiting potential access to systems processing your data to [screened US persons](#). For more information about Azure support for ITAR, see [Azure ITAR compliance offering](#).

DoE 10 CFR Part 810

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's 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 Government can help you meet your DoE 10 CFR Part 810 export control requirements because it's designed to implement specific controls that restrict access to information and systems to [US persons](#) among Azure operations personnel. If you're deploying 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. For more information about Azure support for DoE 10 CFR Part 810, see [Azure DoE 10 CFR Part 810 compliance offering](#).

NRC 10 CFR Part 110

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. Therefore, the **NRC 10 CFR Part 110 regulations wouldn't be applicable** to Azure or Azure Government.

OFAC Sanctions Laws

The [Office of Foreign Assets Control](#) (OFAC) is responsible for administering and enforcing economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries/regions, terrorists, international narcotics traffickers, and those entities engaged in activities related to the proliferation of weapons of mass destruction.

The OFAC defines prohibited transactions as trade or financial transactions and other dealings in which US persons may not engage unless authorized by OFAC or expressly exempt by statute. For web-based interactions, see [FAQ No. 73](#) for general guidance released by OFAC, which specifies, for example, that "Firms that facilitate or engage in e-commerce should do their best to know their customers directly."

As stated in the Microsoft Online Services Terms [Data Protection Addendum](#) (DPA), "Microsoft doesn't control or limit the regions from which customer or customer's end users may access or move customer data." For Microsoft online services, Microsoft conducts due diligence to prevent transactions with entities from OFAC embargoed countries/regions. For example, a sanctions target isn't allowed to provision Azure services. OFAC hasn't issued guidance, like the guidance provided by BIS for the EAR that draws a distinction between cloud service providers and customers when it comes to deemed export. Therefore, it would be **your responsibility to exclude sanctions targets from online transactions** involving your applications, including web sites, deployed on Azure. Microsoft doesn't block network traffic to your web sites deployed on Azure. Even though OFAC mentions that customers can restrict access based in IP table ranges, they also acknowledge that this approach doesn't fully address an internet's firm compliance risks. Therefore, OFAC recommends that e-commerce firms should know their customers directly. Microsoft isn't responsible for and doesn't have the means to know directly the end users that interact with your applications deployed on Azure.

OFAC sanctions are in place to prevent "conducting business with a sanctions target", that is, preventing transactions involving trade, payments, financial instruments, and so on. OFAC sanctions aren't intended to prevent a resident of a proscribed country/region from viewing a public web site.

Managing export control requirements

You should assess carefully how your use of Azure may implicate US export controls, and determine whether any of the data you want to store or process in the cloud may be subject to export controls. Microsoft provides you with contractual commitments, operational processes, and technical features to help you meet your export control obligations when using Azure. The following Azure features are available to help you 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 or country/region. For example, you may therefore ensure that data is stored in the United States or your country/region of choice and minimize transfer of controlled technology/technical data outside the target country/region. Your data isn't *intentionally stored* in a non-conforming location, consistent with the EAR and ITAR rules.
- **End-to-end encryption** – Implies the data is always kept encrypted between the originator and intended recipient, and the means of decryption isn'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](#).

- **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 your data. For those rare instances where resolving your support requests requires elevated access to your data, [Customer Lockbox for Azure](#) puts you in charge of approving or denying data access requests.
- **Tools and protocols to prevent unauthorized deemed export/re-export** – Apart from the EAR and 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 revealed to non-US person who can't read or understand the data while it's encrypted and thus there's 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.

Location of customer data

Microsoft provides [strong customer commitments](#) regarding [cloud services data residency and transfer policies](#). Most Azure services are deployed regionally and enable you to specify the region into which the service will be deployed, for example, United States. This commitment helps ensure that [customer data](#) stored in a US region will remain in the United States and won't be moved to another region outside the United States.

Data encryption

Azure has extensive support to safeguard your data using [data encryption](#), including various encryption models:

- Server-side encryption that uses service-managed keys, customer-managed keys (CMK) in Azure, or CMK in customer-controlled hardware.

- Client-side encryption that enables you to manage and store keys on-premises or in another secure location.

Data encryption provides isolation assurances that are tied directly to encryption key access. Since Azure uses strong ciphers for data encryption, only entities with access to encryption keys can have access to data. Revoking or deleting encryption keys renders the corresponding data inaccessible.

FIPS 140 validated cryptography

The [Federal Information Processing Standard \(FIPS\) 140](#) is a US government standard that defines minimum security requirements for cryptographic modules in information technology products. The current version of the standard, FIPS 140-3, has security requirements covering 11 areas related to the design and implementation of a cryptographic module. Microsoft maintains an active commitment to meeting the [FIPS 140 requirements](#), having validated cryptographic modules since the standard's inception in 2001. Microsoft validates its cryptographic modules under the US National Institute of Standards and Technology (NIST) [Cryptographic Module Validation Program](#) (CMVP). Multiple Microsoft products, including many cloud services, use these cryptographic modules.

While the current CMVP FIPS 140 implementation guidance precludes a FIPS 140 validation for a cloud service, cloud service providers can obtain and operate FIPS 140 validated cryptographic modules for the computing elements that comprise their cloud services. Azure is built with a combination of hardware, commercially available operating systems (Linux and Windows), and Azure-specific version of Windows. Through the Microsoft [Security Development Lifecycle](#) (SDL), all Azure services use FIPS 140 approved algorithms for data security because the operating system uses FIPS 140 approved algorithms while operating at a hyper scale cloud. The corresponding crypto modules are FIPS 140 validated as part of the Microsoft [Windows FIPS validation program](#). Moreover, you can store your own cryptographic keys and other secrets in FIPS 140 validated hardware security modules (HSMs).

Encryption key management

Proper protection and management of encryption keys is essential for data security. [Azure Key Vault](#) is a cloud service for securely storing and managing secrets. Key Vault enables you to store your encryption keys in hardware security modules (HSMs) that are FIPS 140 validated. For more information, see [Data encryption key management](#).

Data encryption in transit

Azure provides many options for [encrypting data in transit](#). Data encryption in transit isolates your network traffic from other traffic and helps protect data from interception. For more information, see [Data encryption in transit](#).

Data encryption at rest

Azure provides extensive options for [encrypting data at rest](#) to help you safeguard your data and meet your compliance needs using both Microsoft-managed encryption keys and customer-managed encryption keys. This process relies on multiple encryption keys and services such as Azure Key Vault and Microsoft Entra ID to ensure secure key access and centralized key management. For more information about Azure Storage encryption and Azure Disk encryption, see [Data encryption at rest](#).

Azure SQL Database provides [transparent data encryption](#) (TDE) at rest by [default](#). TDE performs real-time encryption and decryption operations on the data and log files. Database Encryption Key (DEK) is a symmetric key stored in the database boot record for availability during recovery. It's secured via a certificate stored in the master database of the server or an asymmetric key called TDE Protector stored under your control in [Azure Key Vault](#). Key Vault supports [bring your own key](#) (BYOK), which enables you to store the TDE Protector in Key Vault and control key management tasks including key rotation, permissions, deleting keys, enabling auditing/reporting on all TDE Protectors, and so on. The key can be generated by the Key Vault, imported, or [transferred to the Key Vault from an on-premises HSM device](#). You can also use the [Always Encrypted](#) feature of Azure SQL Database, which is designed specifically to help protect sensitive data by allowing you to encrypt data inside your applications and [never reveal the encryption keys to the database engine](#). In this manner, Always Encrypted provides separation between those users who own the data and can view it and those users who manage the data but should have no access.

Restrictions on insider access

All Azure and Azure Government employees in the United States are subject to Microsoft background checks. For more information, see [Screening](#).

Insider threat is characterized as potential for providing back-door connections and cloud service provider (CSP) privileged administrator access to your systems and data. For more information on how Microsoft restricts insider access to your data, see [Restrictions on insider access](#).

Monitoring your Azure resources

Azure provides essential services that you can use to gain in-depth insight into your provisioned Azure resources and get alerted about suspicious activity, including outside attacks aimed at your applications and data. For more information about these services, see [Customer monitoring of Azure resources](#).

Conclusion

You should carefully assess how your use of Azure may implicate US export controls and determine whether any of the data you want to store or process in the cloud may be subject to export controls. Microsoft Azure provides important technical features, operational processes, and contractual commitments to help you manage export control risks. Where technical data subject to US export controls may be involved, Azure is configured to offer features that help mitigate the potential risk of you inadvertently violating US export controls when accessing controlled technical data in Azure. With appropriate planning, you can use Azure features and your own internal procedures to help ensure full compliance with US export controls when using the Azure platform.

Next steps

To help you navigate export control rules, Microsoft has published the [Microsoft Azure Export Controls](#) whitepaper, which describes US export controls (particularly as they apply to software and technical data), reviews potential sources of export control risks, and offers specific guidance to help you assess your obligations under these controls.

Learn more about:

- [Azure Security](#)
- [Azure Compliance](#)
- [Microsoft government solutions](#)
- [What is Azure Government?](#)
- [Explore Azure Government](#)
- [Exporting Microsoft products](#)
- [Azure Government compliance](#)
- [Azure EAR compliance offering](#)
- [Azure ITAR compliance offering](#)
- [Azure DoE 10 CFR Part 810 compliance offering](#)
- [Azure FedRAMP compliance offering](#)

Details of the CIS Microsoft Azure Foundations Benchmark 1.3.0 (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 CIS Microsoft Azure Foundations Benchmark 1.3.0 (Azure Government). For more information about this compliance standard, see [CIS Microsoft Azure Foundations Benchmark 1.3.0](#). To understand *Ownership*, see [Azure Policy policy definition](#) and [Shared responsibility in the cloud](#).

The following mappings are to the [CIS Microsoft Azure Foundations Benchmark 1.3.0](#) 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 [CIS Microsoft Azure Foundations Benchmark v1.3.0](#) 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](#).

1 Identity and Access Management

Ensure that multi-factor authentication is enabled for all privileged users

ID: CIS Microsoft Azure Foundations Benchmark recommendation 1.1 Ownership: Shared

[+] [Expand table](#)

Name	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 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 ↗

Ensure that multi-factor authentication is enabled for all non-privileged users

ID: CIS Microsoft Azure Foundations Benchmark recommendation 1.2 Ownership: Shared

[+] [Expand table](#)

Name	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 ↗

Ensure guest users are reviewed on a monthly basis

ID: CIS Microsoft Azure Foundations Benchmark recommendation 1.3 Ownership: Shared

[Expand table](#)

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

2 Security Center

Ensure that Azure Defender is set to On for Servers

ID: CIS Microsoft Azure Foundations Benchmark recommendation 2.1 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 ↴

Ensure that 'Automatic provisioning of monitoring agent' is set to 'On'

ID: CIS Microsoft Azure Foundations Benchmark recommendation 2.11 Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)			(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 ↗

Ensure 'Additional email addresses' is configured with a security contact email

ID: CIS Microsoft Azure Foundations Benchmark recommendation 2.13 Ownership: Shared

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

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

Ensure that 'Notify about alerts with the following severity' is set to 'High'

ID: CIS Microsoft Azure Foundations Benchmark recommendation 2.14 Ownership: Shared

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

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

Ensure that Azure Defender is set to On for Azure SQL database servers

ID: CIS Microsoft Azure Foundations Benchmark recommendation 2.3 **Ownership: Shared**

[Expand table](#)

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 ↗

Ensure that Azure Defender is set to On for Storage

ID: CIS Microsoft Azure Foundations Benchmark recommendation 2.5 **Ownership: Shared**

[Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Microsoft Defender for Storage (Classic) should be enabled ↗	Microsoft Defender for Storage (Classic) provides detections of unusual and potentially harmful attempts to access or exploit storage accounts.	AuditIfNotExists, Disabled	1.0.4 ↗

Ensure that Azure Defender is set to On for Kubernetes

ID: CIS Microsoft Azure Foundations Benchmark recommendation 2.6 Ownership: Shared

[+] Expand table

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

Ensure that Azure Defender is set to On for Container Registries

ID: CIS Microsoft Azure Foundations Benchmark recommendation 2.7 Ownership: Shared

[+] Expand table

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

3 Storage Accounts

Ensure that 'Secure transfer required' is set to 'Enabled'

ID: CIS Microsoft Azure Foundations Benchmark recommendation 3.1 Ownership: Shared

[+] Expand table

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Secure transfer to storage	Audit requirement of Secure transfer in your storage account. Secure transfer is an option that forces your	Audit, Deny,	2.0.0 ↴

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
accounts should be enabled ↴	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	Disabled	

Ensure default network access rule for Storage Accounts is set to deny

ID: CIS Microsoft Azure Foundations Benchmark recommendation 3.6 Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
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 using virtual network rules ↴	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 ↴

Ensure 'Trusted Microsoft Services' is enabled for Storage Account access

ID: CIS Microsoft Azure Foundations Benchmark recommendation 3.7 Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)			(GitHub)
Storage accounts should allow access from trusted Microsoft services ↗	Some Microsoft services that interact with storage accounts operate from networks that can't be granted access through network rules. To help this type of service work as intended, allow the set of trusted Microsoft services to bypass the network rules. These services will then use strong authentication to access the storage account.	Audit, Deny, Disabled	1.0.0 ↗

Ensure storage for critical data are encrypted with Customer Managed Key

ID: CIS Microsoft Azure Foundations Benchmark recommendation 3.9 Ownership: Shared

[] Expand table

Name	Description	Effect(s)	Version
(Azure portal)			(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 ↗

4 Database Services

Ensure that 'Auditing' is set to 'On'

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.1.1 Ownership: Shared

[] Expand table

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

Ensure that 'Data encryption' is set to 'On' on a SQL Database

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.1.2 **Ownership: Shared**

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

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

Ensure that 'Auditing' Retention is 'greater than 90 days'

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.1.3 **Ownership: Shared**

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
SQL servers with auditing to storage account destination should be configured with 90 days retention or higher ↴	For incident investigation purposes, we recommend setting the data retention for your SQL Server' auditing to storage account destination to at least 90 days. 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.	AuditIfNotExists, Disabled	3.0.0 ↴

Ensure that Advanced Threat Protection (ATP) on a SQL server is set to 'Enabled'

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.2.1 Ownership: Shared

[] [Expand table](#)

Name	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 ↴

Ensure that Vulnerability Assessment (VA) is enabled on a SQL server by setting a Storage Account

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.2.2 Ownership: Shared

[] [Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
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	1.0.1 ↴
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	3.0.0 ↴

Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.3.1 **Ownership: Shared**

[+] [Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Enforce SSL connection should be enabled for PostgreSQL database servers	<p>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.</p>	Audit, Disabled	1.0.1

Ensure 'Enforce SSL connection' is set to 'ENABLED' for MySQL Database Server

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.3.2 **Ownership: Shared**

[+] [Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Enforce SSL connection should be enabled for MySQL database servers	<p>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.</p>	Audit, Disabled	1.0.1

Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.3.3 **Ownership: Shared**

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Log checkpoints should be enabled for PostgreSQL database servers ↴	This policy helps audit any PostgreSQL databases in your environment without log_checkpoints setting enabled.	AuditIfNotExists, Disabled	1.0.0 ↴

Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.3.4 **Ownership: Shared**

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Log connections should be enabled for PostgreSQL database servers ↴	This policy helps audit any PostgreSQL databases in your environment without log_connections setting enabled.	AuditIfNotExists, Disabled	1.0.0 ↴

Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.3.5 **Ownership: Shared**

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Disconnections should be logged for PostgreSQL database servers. ↴	This policy helps audit any PostgreSQL databases in your environment without log_disconnections enabled.	AuditIfNotExists, Disabled	1.0.0 ↴

Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.3.6 Ownership: Shared

[+] [Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Connection throttling should be enabled for PostgreSQL database servers ↗	This policy helps audit any PostgreSQL databases in your environment without Connection throttling enabled. This setting enables temporary connection throttling per IP for too many invalid password login failures.	AuditIfNotExists, Disabled	1.0.0 ↗

Ensure that Azure Active Directory Admin is configured

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.4 Ownership: Shared

[+] [Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(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 ↗

Ensure SQL server's TDE protector is encrypted with Customer-managed key

ID: CIS Microsoft Azure Foundations Benchmark recommendation 4.5 Ownership: Shared

[+] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
SQL managed instances should use customer-managed keys to encrypt data at rest ↗	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	2.0.0 ↗
SQL servers should use customer-managed keys to encrypt data at rest ↗	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	2.0.1 ↗

5 Logging and Monitoring

Ensure the storage account containing the container with activity logs is encrypted with BYOK (Use Your Own Key)

ID: CIS Microsoft Azure Foundations Benchmark recommendation 5.1.4 Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Storage account containing the container with activity logs must be encrypted with BYOK ↗	This policy audits if the Storage account containing the container with activity logs is encrypted with BYOK. The policy works only if the storage account lies on the same subscription as activity logs by design. More information on Azure Storage encryption at rest can be found here https://aka.ms/azurestoragebyok ↗ .	AuditIfExists, Disabled	1.0.0 ↗

Ensure that logging for Azure KeyVault is 'Enabled'

ID: CIS Microsoft Azure Foundations Benchmark recommendation 5.1.5 **Ownership: Shared**

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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	5.0.0 ↗

Ensure that Activity Log Alert exists for Create Policy Assignment

ID: CIS Microsoft Azure Foundations Benchmark recommendation 5.2.1 **Ownership: Shared**

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An activity log alert should exist for specific Policy operations ↗	This policy audits specific Policy operations with no activity log alerts configured.	AuditIfNotExists, Disabled	3.0.0 ↗

Ensure that Activity Log Alert exists for Delete Policy Assignment

ID: CIS Microsoft Azure Foundations Benchmark recommendation 5.2.2 **Ownership: Shared**

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An activity log alert should exist for specific Policy operations ↗	This policy audits specific Policy operations with no activity log alerts configured.	AuditIfNotExists, Disabled	3.0.0 ↗

Ensure that Activity Log Alert exists for Create or Update Network Security Group

ID: CIS Microsoft Azure Foundations Benchmark recommendation 5.2.3 **Ownership:** Shared

[+] [Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
An activity log alert should exist for specific Administrative operations ↴	This policy audits specific Administrative operations with no activity log alerts configured.	AuditIfNotExists, Disabled	1.0.0 ↴

Ensure that Activity Log Alert exists for Delete Network Security Group

ID: CIS Microsoft Azure Foundations Benchmark recommendation 5.2.4 **Ownership:** Shared

[+] [Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
An activity log alert should exist for specific Administrative operations ↴	This policy audits specific Administrative operations with no activity log alerts configured.	AuditIfNotExists, Disabled	1.0.0 ↴

Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule

ID: CIS Microsoft Azure Foundations Benchmark recommendation 5.2.5 **Ownership:** Shared

[+] [Expand table](#)

Name	Description	Effect(s)	Version
(GitHub)			
An activity log alert should exist for specific	This policy audits specific Administrative operations with no activity log alerts configured.	AuditIfNotExists, Disabled	1.0.0 ↴

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Administrative operations ↗	activity log alerts configured.		

Ensure that activity log alert exists for the Delete Network Security Group Rule

ID: CIS Microsoft Azure Foundations Benchmark recommendation 5.2.6 **Ownership:**
Shared

↔ [Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
An activity log alert should exist for specific Administrative operations ↗	This policy audits specific Administrative operations with no activity log alerts configured.	AuditIfNotExists, Disabled	1.0.0 ↗
Administrative operations ↗			

Ensure that Activity Log Alert exists for Create or Update Security Solution

ID: CIS Microsoft Azure Foundations Benchmark recommendation 5.2.7 **Ownership:**
Shared

↔ [Expand table](#)

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
An activity log alert should exist for specific Security operations ↗	This policy audits specific Security operations with no activity log alerts configured.	AuditIfNotExists, Disabled	1.0.0 ↗
Security operations ↗			

Ensure that Activity Log Alert exists for Delete Security Solution

ID: CIS Microsoft Azure Foundations Benchmark recommendation 5.2.8 **Ownership:**
Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An activity log alert should exist for specific Security operations ↴	This policy audits specific Security operations with no activity log alerts configured.	AuditIfNotExists, Disabled	1.0.0 ↴

Ensure that Activity Log Alert exists for Create or Update or Delete SQL Server Firewall Rule

ID: CIS Microsoft Azure Foundations Benchmark recommendation 5.2.9 Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
An activity log alert should exist for specific Administrative operations ↴	This policy audits specific Administrative operations with no activity log alerts configured.	AuditIfNotExists, Disabled	1.0.0 ↴

Ensure that Diagnostic Logs are enabled for all services which support it.

ID: CIS Microsoft Azure Foundations Benchmark recommendation 5.3 Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↴
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)
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	5.0.0 ↗
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	5.0.0 ↗
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	5.0.0 ↗
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	5.0.0 ↗
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	5.0.0 ↗
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	5.1.0 ↗
Resource logs in Search services 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 ↗
Resource logs in Service Bus 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 ↗

6 Networking

Ensure that Network Watcher is 'Enabled'

ID: CIS Microsoft Azure Foundations Benchmark recommendation 6.5 Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Network Watcher should be enabled ↗	<p>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.</p>	AuditIfNotExists, Disabled	3.0.0 ↗

7 Virtual Machines

Ensure Virtual Machines are utilizing Managed Disks

ID: CIS Microsoft Azure Foundations Benchmark recommendation 7.1 Ownership: Shared

↔ [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
Audit VMs that do not use managed disks ↗	This policy audits VMs that do not use managed disks	audit	1.0.0 ↗

Ensure that 'OS and Data' disks are encrypted with CMK

ID: CIS Microsoft Azure Foundations Benchmark recommendation 7.2 Ownership: Shared

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

Name	Description	Effect(s)	Version
(GitHub)			
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: https://aka.ms/disksse , ↴ Different disk encryption offerings: https://aka.ms/diskencryptioncomparison ↴	AuditIfNotExists, Disabled	2.0.3 ↴

Ensure that only approved extensions are installed

ID: CIS Microsoft Azure Foundations Benchmark recommendation 7.4 Ownership: Shared

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

Name	Description	Effect(s)	Version
(GitHub)			
Only approved VM extensions should be installed ↴	This policy governs the virtual machine extensions that are not approved.	Audit, Deny, Disabled	1.0.0 ↴

Ensure that the latest OS Patches for all Virtual Machines are applied

ID: CIS Microsoft Azure Foundations Benchmark recommendation 7.5 Ownership: Shared

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

Name	Description	Effect(s)	Version
(GitHub)			
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	3.0.0 ↴

Ensure that the endpoint protection for all Virtual Machines is installed

ID: CIS Microsoft Azure Foundations Benchmark recommendation 7.6 Ownership: Shared

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

Name	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	3.1.0 ↗

8 Other Security Considerations

Ensure the key vault is recoverable

ID: CIS Microsoft Azure Foundations Benchmark recommendation 8.4 Ownership: Shared

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

Name	Description	Effect(s)	Version
(GitHub)			
Key vaults should have deletion protection enabled ↗	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	2.1.0 ↗

Enable role-based access control (RBAC) within Azure Kubernetes Services

ID: CIS Microsoft Azure Foundations Benchmark recommendation 8.5 Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
Azure Role-Based Access Control (RBAC) should be used on Kubernetes Services ↗	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	1.0.3 ↗

9 AppService

Ensure App Service Authentication is set on Azure App Service

ID: CIS Microsoft Azure Foundations Benchmark recommendation 9.1 Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
App Service apps should have authentication enabled ↗	Azure App Service Authentication is a feature that can prevent anonymous HTTP requests from reaching the web app, or authenticate those that have tokens before they reach the web app.	AuditIfNotExists, Disabled	2.0.1 ↗
Function apps should have authentication enabled ↗	Azure App Service Authentication is a feature that can prevent anonymous HTTP requests from reaching the Function app, or authenticate those that have tokens before they reach the Function app.	AuditIfNotExists, Disabled	3.0.0 ↗

Ensure FTP deployments are disabled

ID: CIS Microsoft Azure Foundations Benchmark recommendation 9.10 Ownership: Shared

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

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
App Service apps should require FTPS only ↗	Enable FTPS enforcement for enhanced security.	AuditIfNotExists, Disabled	3.0.0 ↗
Function apps should require FTPS only ↗	Enable FTPS enforcement for enhanced security.	AuditIfNotExists, Disabled	3.0.0 ↗

Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service

ID: CIS Microsoft Azure Foundations Benchmark recommendation 9.2 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 ↗

Ensure web app is using the latest version of TLS encryption

ID: CIS Microsoft Azure Foundations Benchmark recommendation 9.3 Ownership: Shared

[] [Expand table](#)

Name (Azure portal)	Description	Effect(s)	Version (GitHub)
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 ↗
Function apps should use the	Periodically, newer versions are released for TLS either due to security flaws, include additional functionality, and enhance speed. Upgrade to the	AuditIfNotExists, Disabled	2.0.1 ↗

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
latest TLS version ↗	latest TLS version for Function apps to take advantage of security fixes, if any, and/or new functionalities of the latest version.		

Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On'

ID: CIS Microsoft Azure Foundations Benchmark recommendation 9.4 Ownership: Shared

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

Name	Description	Effect(s)	Version
(Azure portal)		(GitHub)	
[Deprecated]: Function apps should have 'Client Certificates (Incoming client certificates)' enabled ↗	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	3.1.0-deprecated ↗
App Service apps should have Client Certificates (Incoming client certificates) enabled ↗	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	1.0.0 ↗

Ensure that Register with Azure Active Directory is enabled on App Service

ID: CIS Microsoft Azure Foundations Benchmark recommendation 9.5 Ownership: Shared

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

Name	Description	Effect(s)	Version
(GitHub)			
App Service apps should use managed identity	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	3.0.0
Function apps should use managed identity	Use a managed identity for enhanced authentication security	AuditIfNotExists, Disabled	3.0.0

Ensure that 'HTTP Version' is the latest, if used to run the web app

ID: CIS Microsoft Azure Foundations Benchmark recommendation 9.9 Ownership: Shared

[\[\]](#) Expand table

Name	Description	Effect(s)	Version
(GitHub)			
App Service 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
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

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](#).

Criminal Justice Information Services (CJIS)

Article • 02/02/2023

CJIS overview

The [Criminal Justice Information Services](#) (CJIS) Division of the US Federal Bureau of Investigation (FBI) gives state, local, and federal law enforcement and criminal justice agencies access to criminal justice information (CJI) – for example, fingerprint records and criminal histories. Law enforcement and other government agencies in the United States must ensure that their use of cloud services for the transmission, storage, or processing of CJI complies with the [CJIS Security Policy](#), which establishes minimum security requirements and controls to safeguard CJI.

The CJIS Security Policy integrates presidential and FBI directives, federal laws, and the criminal justice community's Advisory Policy Board decisions, along with guidance from the National Institute of Standards and Technology (NIST). The CJIS Security Policy is updated periodically to reflect evolving security requirements.

In addition to the controls each law enforcement or criminal justice agency is responsible for evaluating, the CJIS Security Policy defines areas that private contractors such as cloud service providers (CSP) must evaluate to determine if their use of cloud services can be consistent with CJIS requirements. These areas correspond closely to control families in [NIST SP 800-53](#), which is also the basis for the US Federal Risk and Authorization Management Program (FedRAMP). The FBI CJIS Information Security Officer (ISO) Program Office has published a [security control mapping of CJIS Security Policy requirements to NIST SP 800-53](#). The corresponding NIST SP 800-53 controls are listed for each CJIS Security Policy section.

A CJIS Security Addendum is a uniform agreement approved by the US Attorney General that helps ensure the security and confidentiality of CJI required by the Security Policy. It commits the contractor to maintaining a security program consistent with federal and state laws, regulations, and standards. The addendum limits the use of CJI to the purposes for which a government agency provided it.

Key updates to CJIS Security Policy in 2022

In October 2022, the CJIS Security Policy was updated to **v5.9.1**, which provided important clarifications for the safeguarding of CJI in a cloud computing environment.

Two areas with significantly updated guidance are related to personnel screening and data encryption with customer managed keys (CMK). For example, Section 5.12.1 *Personnel Screening Requirements for Individuals Requiring Unescorted Access to Unencrypted CJIs* provides important supplemental guidance, as follows:

- Fingerprint-based record checks may not be required for all cloud provider personnel depending upon the type of service offering and access to encryption keys.
- Appendix G.3 was introduced to provide guidance on personnel screening requirements specific to cloud environments.

For cloud computing services that involve the storage, processing, or transmission of CJIs, Section 5.12 security terms and requirements apply to all CSP personnel when their unescorted logical or physical access to any information system results in the ability, right, or privilege to view, modify, or make use of unencrypted CJIs. As described in Section 5.12 for **IaaS and PaaS implementations**, when law enforcement agency maintains sole access to the encryption keys and CSP personnel have no ability, right, or privilege to view, modify, or make use of unencrypted CJIs, then **fingerprint-based background checks may not be required for CSP personnel to comply with the CJIS Security Policy**.

As stated in the CJIS Security Policy Executive Summary regarding the use of data encryption, the essential premise of the CJIS Security Policy is to provide appropriate controls to protect the full lifecycle of CJIs, **whether in transit or at rest**. However, one of the scenarios described in Appendix G.3 *Cloud Computing* states that "since the CJIs are decrypted within the cloud's virtual environment, any administrative personnel employed by the cloud provider having the ability to access the virtual environment must be identified and subjected to security awareness training and personnel security controls as described in the CJIS Security Policy." This reasoning implies that full protection of CJIs in a cloud computing environment that obviates the need for CSP personnel fingerprint-based background checks requires not just data encryption in transit and at rest but also **data encryption in use**, with law enforcement agencies having sole control over encryption keys at every stage. Data encryption in use requires some form of a hardware-based trusted execution environment (TEE), also known as an enclave in confidential computing. With this approach, when data is in the clear, which is needed for efficient data processing in memory, the data is protected inside a TEE with no possibility of unauthorized external access.

In summary, the CJIS Security Policy version 5.9.1 introduced important clarifications for scenarios that require CSP personnel fingerprint-based background checks and placed additional emphasis on the responsibility of agencies to encrypt CJIs in transit, at rest, and in use while maintaining sole control over encryption keys.

ⓘ Important

If you use cloud computing services to store, process, or transmit CJI, then CSP personnel fingerprint-based background checks may not be required to comply with the CJIS Security Policy if you:

- Encrypt CJI in transit, at rest, and in use.
- Maintain sole control over encryption keys, also known as CMK.

There are other important requirements outlined in the CJIS Security Policy, including the need to store and process CJI in the United States. However, with the aforementioned approach, CSP personnel have no logical or physical access to any information system resulting in the ability, right, or privilege to view, modify, or make use of unencrypted CJI.

In December 2022, the CJIS Security Policy [v5.9.2](#) introduced important revisions in Section 5.6 *Identification and Authentication (IA)* and Section 5.15 *System and Information Integrity (SI)* among other changes. Of particular significance to law enforcement and criminal justice agencies using cloud services for the transmission, storage, or processing of CJI are the updated multi-factor authentication (MFA) requirements for identification and authentication of organizational users. For example, MFA is required at Authenticator Assurance Level 2 (AAL2), as described in the National Institute of Standards and Technology (NIST) [SP 800-63](#) *Digital Identity Guidelines*. Moreover, authenticators and verifiers operated at AAL2 shall be validated to meet the requirements of the [Federal Information Processing Standard \(FIPS\) 140](#) *Level 1*.

Azure and CJIS Security Policy

For cloud workloads that must comply with the CJIS Security Policy, Microsoft provides you with a **choice of cloud environments: Azure or Azure Government**. The decision will rest with you based on your business needs.

ⓘ Note

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 NIST [SP 800-53](#) standard, augmented by FedRAMP controls and control enhancements. The areas defined in the CJIS Security Policy correspond closely to control families in NIST SP 800-53. As mentioned previously, the FBI CJIS

Information Security Officer (ISO) Program Office has published a security control mapping of CJIS Security Policy requirements to NIST SP 800-53. The corresponding NIST SP 800-53 controls are listed for each CJIS Security Policy section. Therefore, you can use a FedRAMP audit to gain insight into CSP's control implementation details that are relevant for the CJIS Security Policy requirements. Both Azure and Azure Government maintain a **FedRAMP High Provisional Authorization to Operate (P-ATO)** issued by the FedRAMP Joint Authorization Board (JAB).

Both Azure and Azure Government can help you meet your CJIS Security Policy compliance requirements. These two cloud environments have the same controls for data protection, including the ability to help you maintain sole control over encryption keys when encrypting CJI in transit, at rest, and in use. Both Azure and Azure Government enable you to select United States regions into which CJI and corresponding cloud services will be deployed. For more information about location of customer data, tenant separation, data encryption, multi-factor authentication, restrictions on insider access, and more, see the following guidance document:

- [Azure support for public safety and justice](#)

All Azure and Azure Government employees in the United States are subject to Microsoft background checks. For more information, see [Screening](#). However, Azure operations personnel aren't subject to fingerprint-based background checks mandated by the CJIS Security Policy, so there's extra burden on you to implement CJI encryption that precludes Azure operations personnel access to unencrypted CJI while in transit, at rest, and in use. In contrast, Azure Government provides you with an extra layer of protection through contractual commitments that limit potential access to systems processing your data to screened US persons that have completed fingerprint-based background checks and criminal records checks to address CJIS Security Policy requirements.

Tip

Contact a licensing specialist or your Microsoft account team for access to a Microsoft CJIS customer agreement. Microsoft provides separate CJIS customer agreements for Azure and Azure Government. These agreements specify how certain requirements of the CJIS Security Policy will be fulfilled, what Microsoft responsibilities are, which cloud services are covered, and many other important provisions.

- Learn about [Azure support for public safety and justice](#), including CJIS Security Policy requirements. This article discusses technologies that you can use to safeguard CJI stored or processed in Azure services, including data encryption using Azure Key Vault that enables you to have sole control over encryption keys.
- Learn about the benefits of CJIS support on the Microsoft Cloud: Read how [Genetec cleared criminal investigations](#) using Azure Media Services.

Azure

Azure as a cloud service environment is sometimes referred to as Azure commercial, Azure public, or Azure global. Even though Azure infrastructure is globally distributed, Microsoft provides strong customer commitments regarding [cloud services data residency and transfer policies](#). Most Azure services are deployed regionally and enable you to specify the region into which the service will be deployed, for example, United States. This commitment helps ensure that CJI stored in a US region will remain in the United States and won't be moved to another region outside the United States.

The CJIS Security Policy v5.9.1 updates released in October 2022 indicate that state, local, and federal law enforcement and criminal justice agencies can meet the policy requirements through technical controls under their purview. Consequently, you can use Azure for CJI workloads and not have to rely on fingerprint-based background checks for CSP personnel if you can encrypt CJI during all data lifecycle stages – in transit, at rest, and in use – while maintaining sole control over encryption keys. **You are wholly responsible for the implementation and management of these technical controls to support your compliance with the CJIS Security Policy.** For more information, see [Azure support for public safety and justice](#).

Azure Government

Microsoft will sign the CJIS Security Addendum in states with CJIS Management Agreements to support the use of **Microsoft government cloud** solutions. These agreements tell state law enforcement authorities responsible for compliance with CJIS Security Policy how Microsoft cloud security controls help protect the full lifecycle of data and ensure appropriate background screening of operations personnel with potential access to CJI.

Microsoft has agreements signed with nearly all 50 states and the District of Columbia except for the following states: Delaware, Louisiana, Ohio, South Dakota, and Wyoming. Microsoft continues to work with these state governments to enter into CJIS Management Agreements. The FBI doesn't certify cloud services for compliance with CJIS Security Policy requirements. Instead, a Microsoft attestation is included in

agreements between Microsoft and a state's CJIS authority, and between Microsoft and its customers.

Microsoft's commitment to meeting the applicable CJIS regulatory controls help criminal justice organizations be compliant with the CJIS Security Policy when implementing cloud-based solutions. Based on the signed CJIS Management Agreements, Microsoft can accommodate customers subject to the CJIS Security Policy requirements in:

- [Azure Government](#)
- [Dynamics 365 US Government](#)
- [Office 365 GCC](#)

Microsoft has assessed the operational policies and procedures of Microsoft Azure Government, Dynamics 365 US Government, and Office 365 GCC, and will attest to their ability in the applicable services agreements to meet FBI requirements. **These cloud environments maintain fingerprint-based background checks on operations personnel with potential access to unencrypted CJI.**

Applicability

- Azure
- Azure Government

Office 365 and CJIS

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

Frequently asked questions

Where can I request compliance information?

Contact your Microsoft account representative for information on the jurisdiction you are interested in. Contact cjis@microsoft.com for information on which services are currently available in your state.

How does Microsoft demonstrate that its cloud services enable compliance with my state's requirements?

For both Azure and Azure Government, see [Azure support for public safety and justice](#) for guidance on how to encrypt CJI and retain sole control over encryption keys to address key CJIS Security Policy requirements. Moreover, for Azure Government, Microsoft has signed the CJIS Management Agreements with state CJIS Systems Agencies (CSA) in nearly all 50 states – you may request a copy from your state's CSA.

Microsoft also provides you with in-depth security, privacy, and compliance information. For example, you can review audit reports prepared by independent, third-party auditors. These audit reports validate that Microsoft has implemented security controls (such as the NIST SP 800-53 controls) appropriate to the relevant audit scope. A good place to start would be the Azure [FedRAMP compliance offering](#).

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 NIST [SP 800-53](#) standard, augmented by FedRAMP controls and control enhancements. Both Azure and Azure Government maintain a [FedRAMP High](#) Provisional Authorization to Operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB).

I am using Azure Government for my CJI workloads. Does that mean that I don't have to worry about CJI safeguarding?

No. Azure Government gives you extra assurances and peace of mind through contractual commitments regarding storage of your data in the United States and limiting potential access to systems processing your data to screened US persons that have completed fingerprint-based background checks and criminal records checks to address CJIS Security Policy requirements. However, you still need to address the CJIS Security Policy requirements regarding CJI protection.

My state doesn't have a CJIS Management Agreement signed with Microsoft. What should I do?

You can use either Azure or Azure Government for your CJI workloads but in either case you would need to ensure that CJI is encrypted while in transit, at rest, and in use with encryption keys under your exclusive control at all times. See [Azure support for public safety and justice](#) for guidance on how to encrypt CJI and maintain sole control over encryption keys. Per the updated CJIS Security Policy v5.9.1, if you encrypt CJI in transit, at rest, and in use while maintaining sole control over encryption keys, the CSP personnel fingerprint-based background checks may not be required to comply with the CJIS Security Policy.

Do I need to use confidential computing VMs for IaaS workloads involving CJI?

- Yes, for Azure.
- Yes, for Azure Government in states that haven't signed a CJIS Management Agreement with Microsoft.
- No, for Azure Government in states with signed CJIS Management Agreements.

Our reading of the updated CJIS Security Policy v5.9.1 Appendix G.3 *Cloud Computing* indicates that the policy is aiming for absolute assurances that CSP personnel can never access the virtualized environment if the requirement for fingerprint-based background

checks on CSP personnel were to be removed. Azure doesn't mandate fingerprint-based background checks for operations personnel whereas Azure Government does. Therefore, to ensure compliance with the CJIS Security Policy in Azure, you need to encrypt CJI while in use and maintain sole ownership of encryption keys. The risk of Azure operations personnel access to unencrypted CJI is extraordinarily low as explained in [Restrictions on insider access](#) even for guest VM memory crash dumps. Nonetheless, when data is loaded into VM memory for processing, it must be in the clear and the most expedient way to safeguard access with certainty is via [confidential computing](#) VMs, which protect data in a hardware-based trusted execution environment (TEE), also known as an enclave.

Where do I start with my agency's compliance effort?

The [CJIS Security Policy](#) covers the requirements that your agency must address to protect CJI. In addition, your Microsoft account representative can put you in touch with Microsoft subject matter experts familiar with the requirements of your jurisdiction.

Resources

- [Azure compliance documentation](#)
- [Azure enables a world of compliance](#)
- [Microsoft 365 compliance offerings](#)
- [Compliance on the Microsoft Trust Center](#)
- [Microsoft government solutions](#)
- [Microsoft for public safety and justice](#)
- [Criminal Justice Information Services \(CJIS\)](#)
- [CJIS Security Policy](#)
- [NIST SP 800-53 Security and Privacy Controls for Information Systems and Organizations](#)
- [Azure FedRAMP compliance offering](#)
- [Azure StateRAMP compliance offering](#)

Department of Defense (DoD) in Azure Government

Article • 05/09/2023

Overview

Azure Government is used by the US Department of Defense (DoD) entities to deploy a broad range of workloads and solutions. Some of these workloads can be subject to the DoD Cloud Computing [Security Requirements Guide](#) (SRG) Impact Level 4 (IL4) and Impact Level 5 (IL5) restrictions. Azure Government was the first hyperscale cloud services platform to be awarded a DoD IL5 Provisional Authorization (PA) by the Defense Information Systems Agency (DISA). For more information about DISA and DoD IL5, see [Department of Defense \(DoD\) Impact Level 5](#) compliance documentation.

Azure Government offers the following regions to DoD mission owners and their partners:

Regions	Relevant authorizations	# of IL5 PA services
US Gov Arizona	FedRAMP High, DoD IL4, DoD IL5	150
US Gov Texas		
US Gov Virginia		
US DoD Central	DoD IL5	60
US DoD East		

Azure Government regions US Gov Arizona, US Gov Texas, and US Gov Virginia (**US Gov regions**) are intended for US federal (including DoD), state, and local government agencies, and their partners. Azure Government regions US DoD Central and US DoD East (**US DoD regions**) are reserved for exclusive DoD use. Separate DoD IL5 PAs are in place for US Gov regions vs. US DoD regions. For service availability in Azure Government, see [Products available by region](#).

The primary differences between DoD IL5 PAs that are in place for US Gov regions vs. US DoD regions are:

- **IL5 compliance scope:** US Gov regions have many more services authorized provisionally at DoD IL5, which in turn enables DoD mission owners and their partners to deploy more realistic applications in these regions.
 - For a complete list of services in scope for DoD IL5 PA in US Gov regions, see [Azure Government services by audit scope](#).

- For a complete list of services in scope for DoD IL5 in US DoD regions, see [US DoD regions IL5 audit scope](#) in this article.
- **IL5 configuration:** US DoD regions are reserved for exclusive DoD use. Therefore, no extra configuration is needed in US DoD regions when deploying Azure services intended for IL5 workloads. In contrast, some Azure services deployed in US Gov regions require extra configuration to meet DoD IL5 compute and storage isolation requirements, as explained in [Isolation guidelines for Impact Level 5 workloads](#).

Note

If you are subject to DoD IL5 requirements, we recommend that you prioritize US Gov regions for your workloads, as follows:

- **New deployments:** Choose US Gov regions for your new deployments. Doing so will allow you to benefit from the latest cloud innovations while meeting your DoD IL5 isolation requirements.
- **Existing deployments:** If you have existing deployments in US DoD regions, we encourage you to migrate these workloads to US Gov regions to take advantage of additional services.

Azure provides [extensive support for tenant isolation](#) across compute, storage, and networking services to segregate each customer's applications and data. This approach provides the scale and economic benefits of multi-tenant cloud services while rigorously helping prevent other customers from accessing your data or applications.

Hyper-scale cloud also offers a feature-rich environment incorporating the latest cloud innovations such as artificial intelligence, machine learning, IoT services, intelligent edge, and many more to help DoD mission owners implement their mission objectives. Using Azure Government cloud capabilities, you benefit from rapid feature growth, resiliency, and the cost-effective operation of the hyper-scale cloud while still obtaining the levels of isolation, security, and confidence required to handle workloads subject to FedRAMP High, DoD IL4, and DoD IL5 requirements.

US Gov regions IL5 audit scope

For a complete list of services in scope for DoD IL5 PA in US Gov regions (US Gov Arizona, US Gov Texas, and US Gov Virginia), see [Azure Government services by audit scope](#).

US DoD regions IL5 audit scope

The following services are in scope for DoD IL5 PA in US DoD regions (US DoD Central and US DoD East):

- [API Management](#) ↗
- [Application Gateway](#) ↗
- [Microsoft Entra ID \(Free\)](#)
- [Microsoft Entra ID \(P1 + P2\)](#)
- [Azure Analysis Services](#) ↗
- [Azure Backup](#) ↗
- [Azure Cache for Redis](#) ↗
- [Azure Cloud Services](#) ↗
- [Azure Cosmos DB](#) ↗
- [Azure Database for MySQL](#) ↗
- [Azure Database for PostgreSQL](#) ↗
- [Azure DNS](#) ↗
- [Azure ExpressRoute](#) ↗
- [Azure Firewall](#) ↗
- [Azure Front Door](#) ↗
- [Azure Functions](#) ↗
- [Azure HDInsight](#) ↗
- [Azure Lab Services](#) ↗
- [Azure Logic Apps](#) ↗
- [Azure Managed Applications](#) ↗
- [Azure Media Services](#) ↗
- [Azure Monitor](#) ↗
- [Azure Resource Manager](#) ↗
- [Azure Scheduler \(replaced by Azure Logic Apps\)](#) ↗
- [Azure Service Fabric](#) ↗
- [Azure Service Manager \(RDFE\)](#)
- [Azure Site Recovery](#) ↗
- [Azure SQL Database](#) ↗
- [Azure Synapse Analytics](#) ↗
- [Batch](#) ↗
- [Dynamics 365 Customer Engagement](#)
- [Event Grid](#) ↗
- [Event Hubs](#) ↗
- [Import/Export](#) ↗
- [Key Vault](#) ↗
- [Load Balancer](#) ↗

- Microsoft Azure portal [↗](#)
- Microsoft Defender for Endpoint (formerly Microsoft Defender Advanced Threat Protection)
- Microsoft Graph
- Microsoft Stream
- Network Watcher [↗](#)
- Power Apps
- Power Apps portal [↗](#)
- Power Automate (formerly Microsoft Flow)
- Power BI [↗](#)
- Power BI Embedded [↗](#)
- Service Bus [↗](#)
- SQL Server Stretch Database [↗](#)
- Storage: Blobs [↗](#) (incl. Azure Data Lake Storage Gen2)
- Storage: Disks [↗](#) (incl. managed disks)
- Storage: Files [↗](#)
- Storage: Queues [↗](#)
- Storage: Tables [↗](#)
- Traffic Manager [↗](#)
- Virtual Machine Scale Sets [↗](#)
- Virtual Machines [↗](#)
- Virtual Network [↗](#)
- VPN Gateway [↗](#)
- Web Apps (App Service) [↗](#)

Frequently asked questions

What are the US DoD regions?

Azure Government regions US DoD Central and US DoD East (US DoD regions) are physically separated Azure Government regions reserved for exclusive use by the DoD. They reside on the same isolated network as Azure Government regions US Gov Arizona, US Gov Texas, and US Gov Virginia (US Gov regions) and use the same identity model. Both the network and identity model are separate from Azure commercial.

What is the difference between US Gov regions and US DoD regions?

Azure Government is a US government community cloud providing services for federal, state and local government customers, tribal entities, and other entities subject to various US government regulations such as CJIS, ITAR, and others. All Azure Government regions are designed to meet the security requirements for DoD IL5 workloads. They're deployed on a separate and isolated network and use a separate identity model from Azure commercial regions. US DoD regions achieve DoD IL5 tenant separation requirements by being dedicated exclusively to DoD. In US Gov regions, some services require extra configuration to meet DoD IL5 compute and storage isolation requirements, as explained in [Isolation guidelines for Impact Level 5 workloads](#).

How do US Gov regions support IL5 data?

Azure provides [extensive support for tenant isolation](#) across compute, storage, and networking services to segregate each customer's applications and data. This approach provides the scale and economic benefits of multi-tenant cloud services while rigorously helping prevent other customers from accessing your data or applications. Some Azure services deployed in US Gov regions require extra configuration to meet DoD IL5 compute and storage isolation requirements, as explained in [Isolation guidelines for Impact Level 5 workloads](#).

What is IL5 data?

IL5 accommodates controlled unclassified information (CUI) that requires a higher level of protection than is afforded by IL4 as deemed necessary by the information owner, public law, or other government regulations. IL5 also supports unclassified National Security Systems (NSS). This impact level accommodates NSS and CUI categorizations based on CNSSI 1253 up to moderate confidentiality and moderate integrity (M-M-x). For more information on IL5 data, see [DoD IL5 overview](#).

What is the difference between IL4 and IL5 data?

IL4 data is controlled unclassified information (CUI) that may include data subject to export control, protected health information, and other data requiring explicit CUI designation (for example, For Official Use Only, Law Enforcement Sensitive, and Sensitive Security Information).

IL5 data includes CUI that requires a higher level of protection as deemed necessary by the information owner, public law, or government regulation. IL5 data is inclusive of unclassified National Security Systems.

Do Azure Government regions support classified data such as IL6?

No. Azure Government regions support only unclassified data up to and including IL5. In contrast, [IL6 data](#) is defined as classified information up to Secret, and can be accommodated in [Azure Government Secret](#).

What DoD organizations can use Azure Government?

All Azure Government regions are built to support DoD customers, including:

- The Office of the Secretary of Defense
- The Joint Chiefs of Staff
- The Joint Staff
- The Defense Agencies
- Department of Defense Field Activities
- The Department of the Army
- The Department of the Navy (including the United States Marine Corps)
- The Department of the Air Force
- The United States Coast Guard
- The unified combatant commands
- Other offices, agencies, activities, and commands under the control or supervision of any approved entity named above

What services are available in Azure Government?

For service availability in Azure Government, see [Products available by region](#).

What services are part of your IL5 authorization scope?

For a complete list of services in scope for DoD IL5 PA in US Gov regions, see [Azure Government services by audit scope](#). For a complete list of services in scope for DoD IL5 PA in US DoD regions, see [US DoD regions IL5 audit scope](#) in this article.

Next steps

- [Acquiring and accessing Azure Government](#)
- [How to buy Azure Government](#)
- [Get started with Azure Government](#)
- [Azure Government Blog](#)

- Azure Government security
- Azure Government services by audit scope
- Isolation guidelines for Impact Level 5 workloads
- DoD Impact Level 4
- DoD Impact Level 5
- DoD Impact Level 6

Department of Defense (DoD) Impact Level 2 (IL2)

Article • 04/05/2023

DoD IL2 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.

IL2 data includes non-controlled unclassified information, which is all data cleared for public release and some low confidentiality unclassified information that is not designated as controlled unclassified information (CUI). This impact level accommodates non-CUI categorization based on [CNSSI 1253](#) *Security Categorization and Control Selection for National Security Systems* up to low confidentiality and moderate integrity (L-M-x).

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 IL2 information may be hosted in a CSO that minimally holds a FedRAMP Moderate or High provisional authorization, subject to compliance with the personnel security requirements outlined in Section 5.6.2. Only FedRAMP Moderate or High baseline controls will be assessed for DoD IL2 PAs. For an IL2 PA, DoD allows full

reciprocity with FedRAMP Moderate or High provisional authorization to operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB). However, this approach does not relieve the CSP from meeting other security and integration requirements as required by the mission owner. According to Section 5.2.2.1 *Impact Level 2 Location and Separation Requirements* of the Cloud Computing SRG, DoD IL2 PA is adequately covered by a FedRAMP Moderate provisional authorization such that the requirements will not be extra assessed for an IL2 PA.

Azure and DoD IL2

Both Azure and Azure Government maintain a FedRAMP High provisional authorization to operate (P-ATO) issued by the FedRAMP Joint Authorization Board (JAB). According to the FedRAMP Security Controls Baseline (available from [FedRAMP documents](#)), the FedRAMP High baseline encompasses all controls in the FedRAMP Moderate baseline. Both Azure and Azure Government maintain a DoD IL2 PA, which covers non-controlled unclassified information including all data cleared for public release, for the in-scope services.

Applicability

- Azure
- Azure Government

Services in scope

- Azure services in scope for DoD IL2 PA reflect the Azure FedRAMP High P-ATO scope.
- Azure Government services in scope for DoD IL2 PA reflect the Azure Government FedRAMP High P-ATO scope.

For more information, see [Cloud services in audit scope](#).

Office 365 and DoD IL2

For more information about Office 365 compliance, see [Office 365 DoD IL2 documentation](#).

Attestation documents

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

Frequently asked questions

What Azure services are covered by DoD IL2 PA and in what regions?

To find out what services are available in Azure and Azure Government, see [Products available by region](#). For a list of services provisionally authorized at DoD IL2, 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](#)
- [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*
- [DoD Instruction 8510.01](#) *DoD Risk Management Framework (RMF) for DoD Information Technology (IT)*
- [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](#)

Department of Defense (DoD) Impact Level 4 (IL4)

Article • 04/05/2023

DoD IL4 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 3.1.2 (Page 18) of the [Cloud Computing SRG](#), IL4 information covers controlled unclassified information (CUI), non-CUI information, non-critical mission information, and non-national security systems. 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

IL4 accommodates CUI categorizations based on the [Committee on National Security Systems Instruction No. 1253](#) (CNSSI 1253) *Security Categorization and Control Selection for National Security Systems* up to moderate confidentiality and moderate integrity (M-M-x). 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.

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 will be accepted for a DoD IL4 PA without an assessment of extra controls and control enhancements (C/CE); however, assessment of non-C/CE based requirements in the Cloud Computing SRG is needed.

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 IL4

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

For extra customer assistance, Microsoft provides the Azure Policy regulatory compliance built-in initiative for Azure Government, which maps to DoD IL4 **compliance domains** and **controls**:

- DoD IL4 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 IL4 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 IL4 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](#).

Attestation documents

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

Contact DISA for access to the most recent Azure Government DoD IL4 PA letter.

Frequently asked questions

What Azure services are covered by DoD IL4 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 IL4, see [Cloud services in audit scope](#).