Microsoft Security

Microsoft Defender for Cloud

Protect your multicloud and hybrid environments

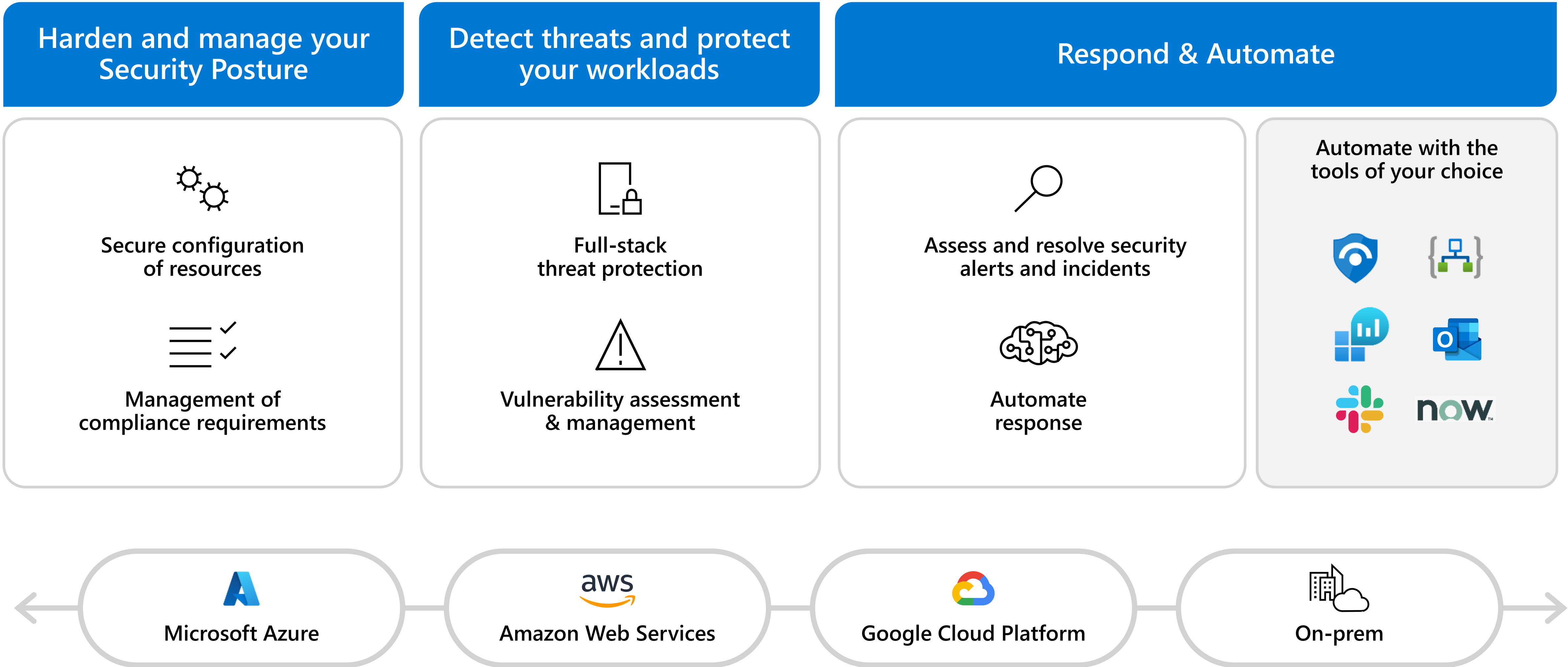
Cloud Security Posture Management
Regulatory Compliance

Brian Stockbrugger
Security Architect

GPSUS

Microsoft Defender For Cloud

Cloud native application protection across clouds and on-prem environments



Harden and manage your Security Posture

Secure configuration of resources

Management of compliance requirements

Detect threats and protect your workloads

Full-stack threat protection

Vulnerability assessment & management

Respond & Automate

Assess and resolve security alerts and incidents

Automate response

Automate with the tools of your choice

Microsoft Azure

Amazon Web Services

Google Cloud Platform

On-prem

Holistic management of your security posture in the cloud

Resource visibility

View and manage your cloud resource inventory

Secure Score

Understand the bottom line of your security posture, implement recommendations, and monitor over time

Compliance

Ensure your configurations align with key compliance standards and enforce organizational policies

Data security

Identify sensitive data and prioritize critical resources

The security dashboard

Centralized posture view

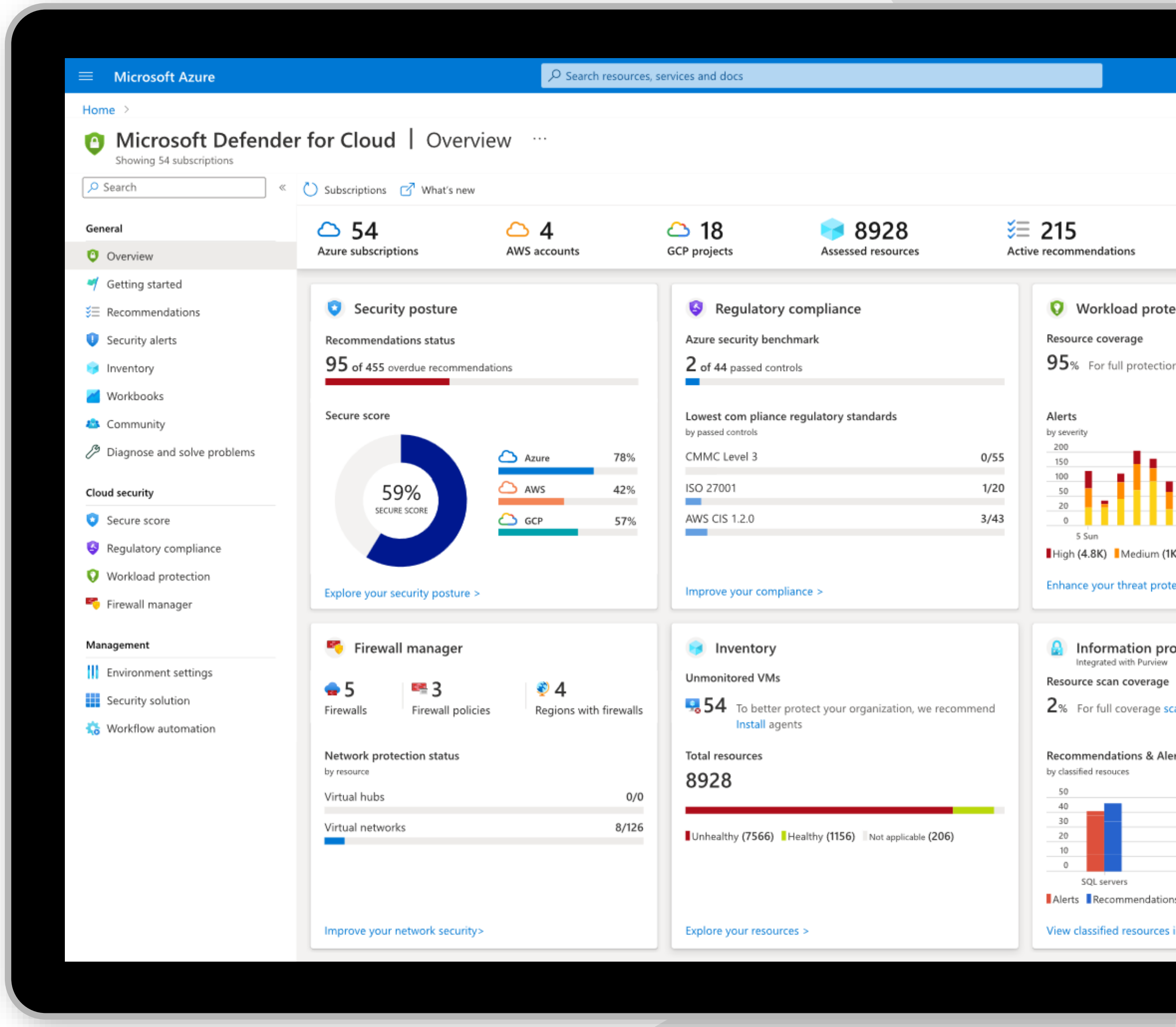
- → Your security posture across Azure, AWS, and GCP in one place

Focused views

- → Easily access deep dive views for security posture, resource inventory, workload protection, and more

Top insights front and center

- → Understand which recommendations to prioritize
- → See your most attacked resources and take action



Microsoft Defender for Cloud | Overview ···

Showing 54 subscriptions

54 Azure subscriptions

4 AWS accounts

18 GCP projects

8928 Assessed resources

215 Active recommendations

Security posture

Recommendations status

95 of 455 overdue recommendations

Secure score

59% SECURE SCORE

Azure	78%
AWS	42%
GCP	57%

Explore your security posture >

Regulatory compliance

Azure security benchmark

2 of 44 passed controls

Lowest com pliance regulatory standards

by passed controls

CMMC Level 3	0/55
ISO 27001	1/20
AWS CIS 1.2.0	3/43

Improve your compliance >

Workload prote

Resource coverage

95% For full protectior

Alerts

by severity

High (4.8K) Medium (1K

Enhance your threat prote

Firewall manager

5 Firewalls

3 Firewall policies

4 Regions with firewalls

Network protection status

by resource

Virtual hubs	0/0
Virtual networks	8/126

Improve your network security>

Inventory

Unmonitored VMs

54 To better protect your organization, we recommend Install agents

Total resources

8928

Unhealthy (7566) Healthy (1156) Not applicable (206)

Explore your resources >

Information pro

Integrated with Purview

Resource scan coverage

2% For full coverage sca

Recommendations & Aler

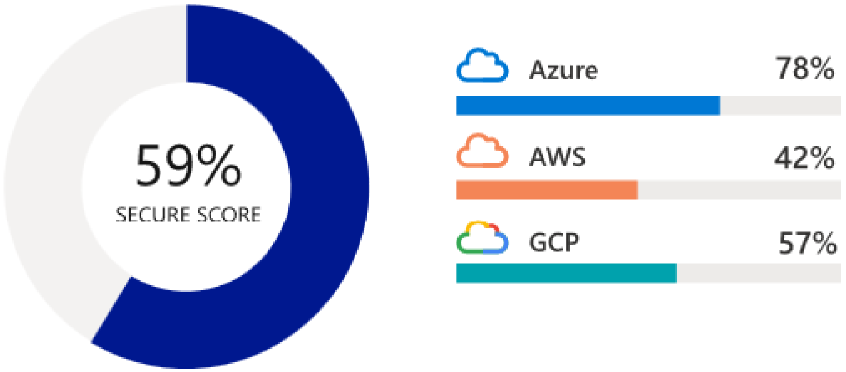
by classified resouces

Alerts Recommendation

View classified resources i

Secure Score

- Assess and implement best practices for security and compliance
- Cover all critical cloud resources across network, access, compute, databases, your service layer and more
- 450+out-of-the-box recommendations
- Create custom recommendations to meet organizational requirements
- Use “Quick fix” to remediate with a single click or scale enforcement mechanisms to enforce policies to avoid configuration drifts



Evaluated categories

Access

Compute

SQL server

IoT

Network

App Services

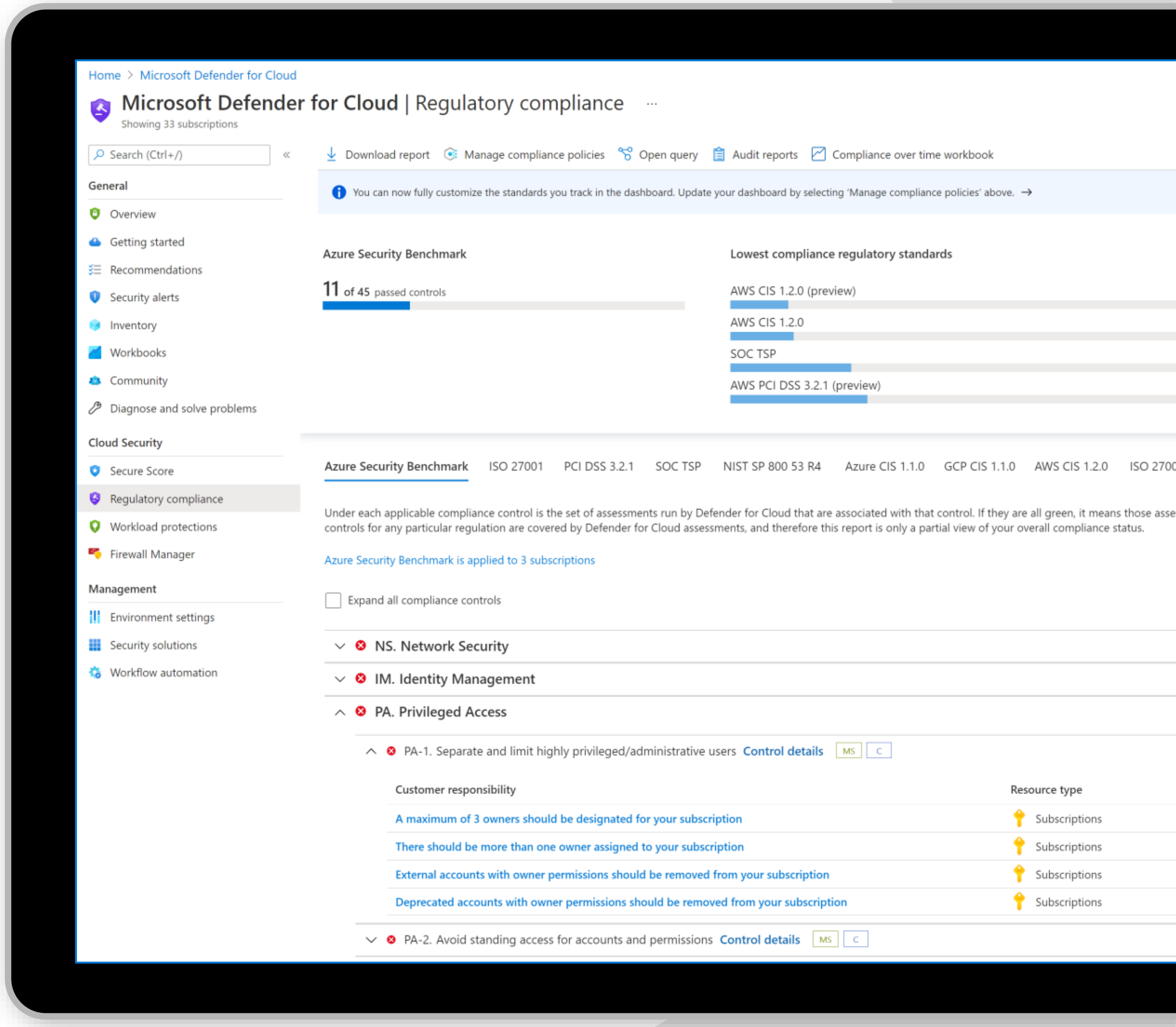
Containers

Compliance assessment and management

- → Assess and manage your compliance status with a continuous assessment of your cloud resources
- → Use industry standards, regulatory compliance frameworks, and vendor provided benchmarks to implement security and compliance best practices
- → Create custom recommendations to meet unique organizational needs

<u>**Support for:**</u>

- ✓ CIS
- ✓ PCI
- ✓ NIST
- ✓ SOC
- ✓ ISO
- ✓ HIPAA
- ✓ Local/National compliance standards
- ✓ Azure Security Benchmark
- ✓ AWS Foundational Security best practices



You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above. →

Azure Security Benchmark

11 of 45 passed controls

Lowest compliance regulatory standards

- AWS CIS 1.2.0 (preview)
- AWS CIS 1.2.0
- SOC TSP
- AWS PCI DSS 3.2.1 (preview)

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those asse controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to 3 subscriptions

☐ Expand all compliance controls

- NS. Network Security
- IM. Identity Management
- PA. Privileged Access
  - PA-1. Separate and limit highly privileged/administrative users Control details MS C

Customer responsibility	Resource type
A maximum of 3 owners should be designated for your subscription	Subscriptions
There should be more than one owner assigned to your subscription	Subscriptions
External accounts with owner permissions should be removed from your subscription	Subscriptions
Deprecated accounts with owner permissions should be removed from your subscription	Subscriptions

  - PA-2. Avoid standing access for accounts and permissions Control details MS C

Azure Security Benchmark

- Azure's own security control framework based on industry standards enables customers to meet their security control requirements in Azure
- Bringing consistency of security capabilities across all Azure Offers using Azure Security Benchmark

Publish

Define and Publish the Benchmark

Azure Security Benchmarks documentation

Standardize

Ensure all Azure Offers meet the Cloud Security Benchmark

Monitor

Automate Benchmark management using Microsoft Defender for Cloud

Importance of security Benchmarks

- Compliance and security baselines critical for successful cloud migration and adoption

Many organizations rely on the CIS/NIST Controls security best practices to improve their cyber defenses

Compliance controls require that standard security controls are measured via configuration baselines

Security configurations that result in breaches are driving awareness to the requirements

Industry standards

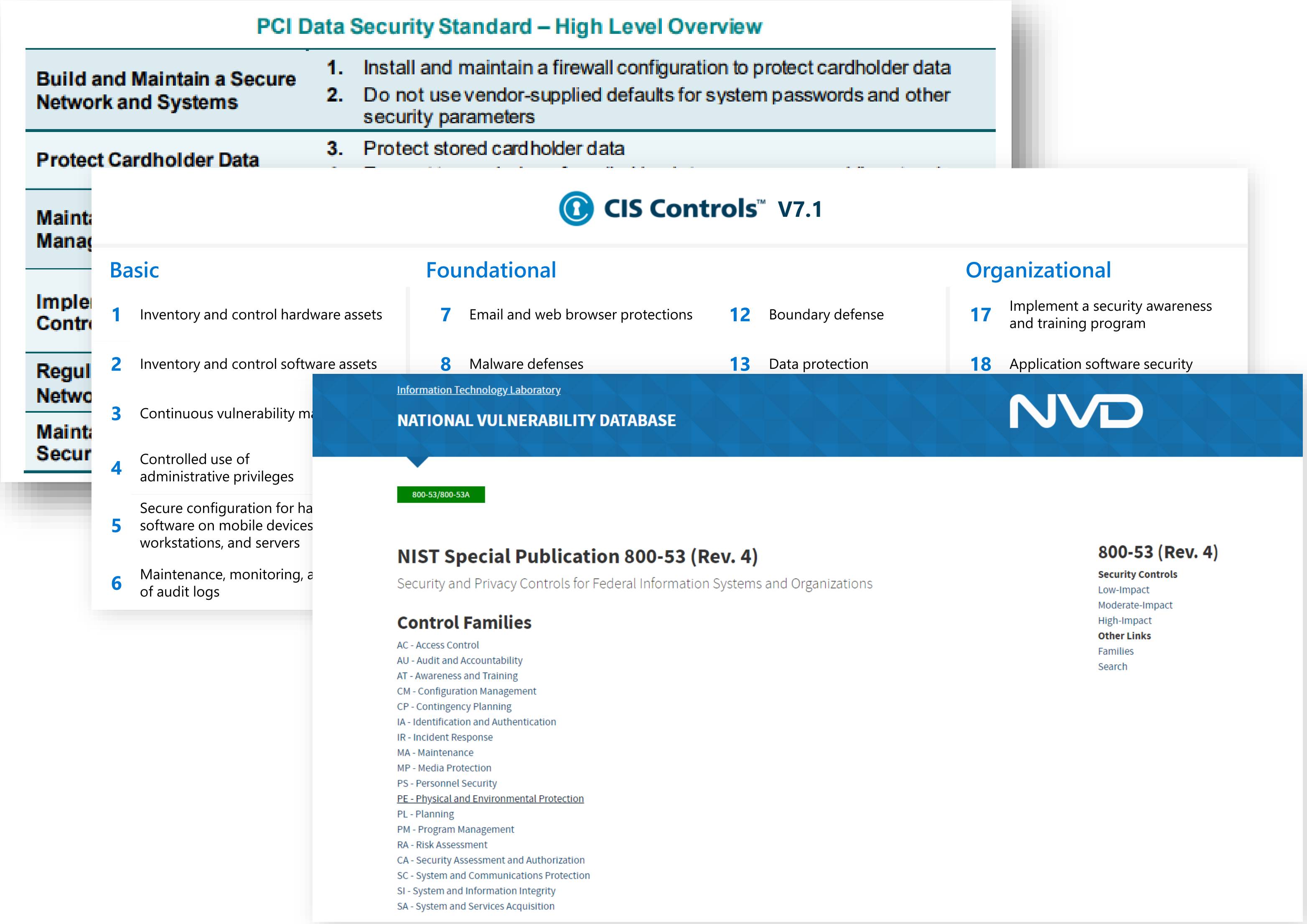
CIS Center for Internet Security®
Confidence in the Connected World

NIST National Institute of Standards and Technology
U.S. Department of Commerce
NIST Special Publication 800-53
[CM-2 Baseline Configuration]

PCI Security Standards Council®

Publish the Benchmark

Making this easier on customers, we've done the translation ourselves



PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
Maint Manag	
Imple Contr	
Regul Netwo	
Maint Secur	

CIS Controls™ V7.1

Basic

1 Inventory and control hardware assets

2 Inventory and control software assets

3 Continuous vulnerability ma

4 Controlled use of administrative privileges

5 Secure configuration for ha software on mobile devices workstations, and servers

6 Maintenance, monitoring, a of audit logs

Foundational

7 Email and web browser protections

8 Malware defenses

12 Boundary defense

13 Data protection

Organizational

17 Implement a security awareness and training program

18 Application software security

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NVD

800-53/800-53A

NIST Special Publication 800-53 (Rev. 4)

Security and Privacy Controls for Federal Information Systems and Organizations

Control Families

- AC - Access Control
- AU - Audit and Accountability
- AT - Awareness and Training
- CM - Configuration Management
- CP - Contingency Planning
- IA - Identification and Authentication
- IR - Incident Response
- MA - Maintenance
- MP - Media Protection
- PS - Personnel Security
- PE - Physical and Environmental Protection
- PL - Planning
- PM - Program Management
- RA - Risk Assessment
- CA - Security Assessment and Authorization
- SC - System and Communications Protection
- SI - System and Information Integrity
- SA - System and Services Acquisition

800-53 (Rev. 4)

Security Controls

Low-Impact

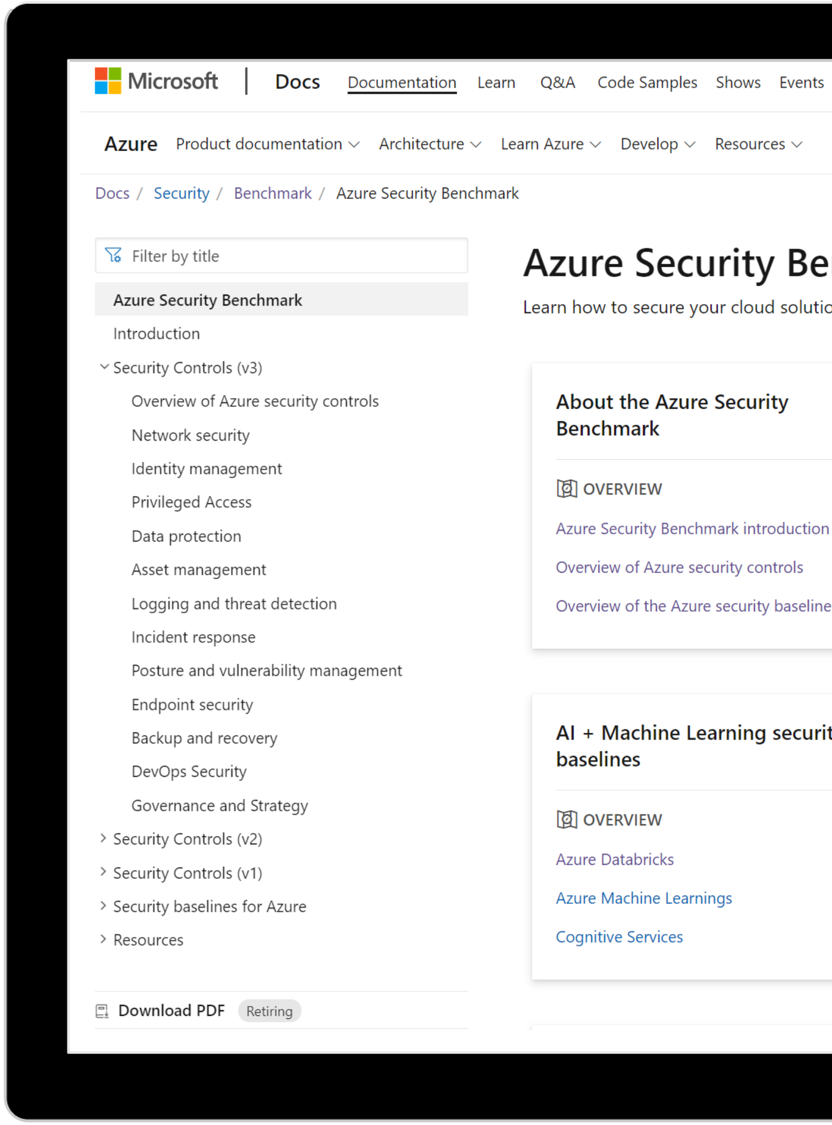
Moderate-Impact

High-Impact

Other Links

Families

Search



Docs / Security / Benchmark / Azure Security Benchmark

Filter by title

- Azure Security Benchmark
- Introduction
- Security Controls (v3)
  - Overview of Azure security controls
  - Network security
  - Identity management
  - Privileged Access
  - Data protection
  - Asset management
  - Logging and threat detection
  - Incident response
  - Posture and vulnerability management
  - Endpoint security
  - Backup and recovery
  - DevOps Security
  - Governance and Strategy
- Security Controls (v2)
- Security Controls (v1)
- Security baselines for Azure
- Resources

Download PDF Retiring

Azure Security Be

Learn how to secure your cloud solutic

About the Azure Security Benchmark

OVERVIEW

Azure Security Benchmark introduction

Overview of Azure security controls

Overview of the Azure security baseline

AI + Machine Learning securit baselines

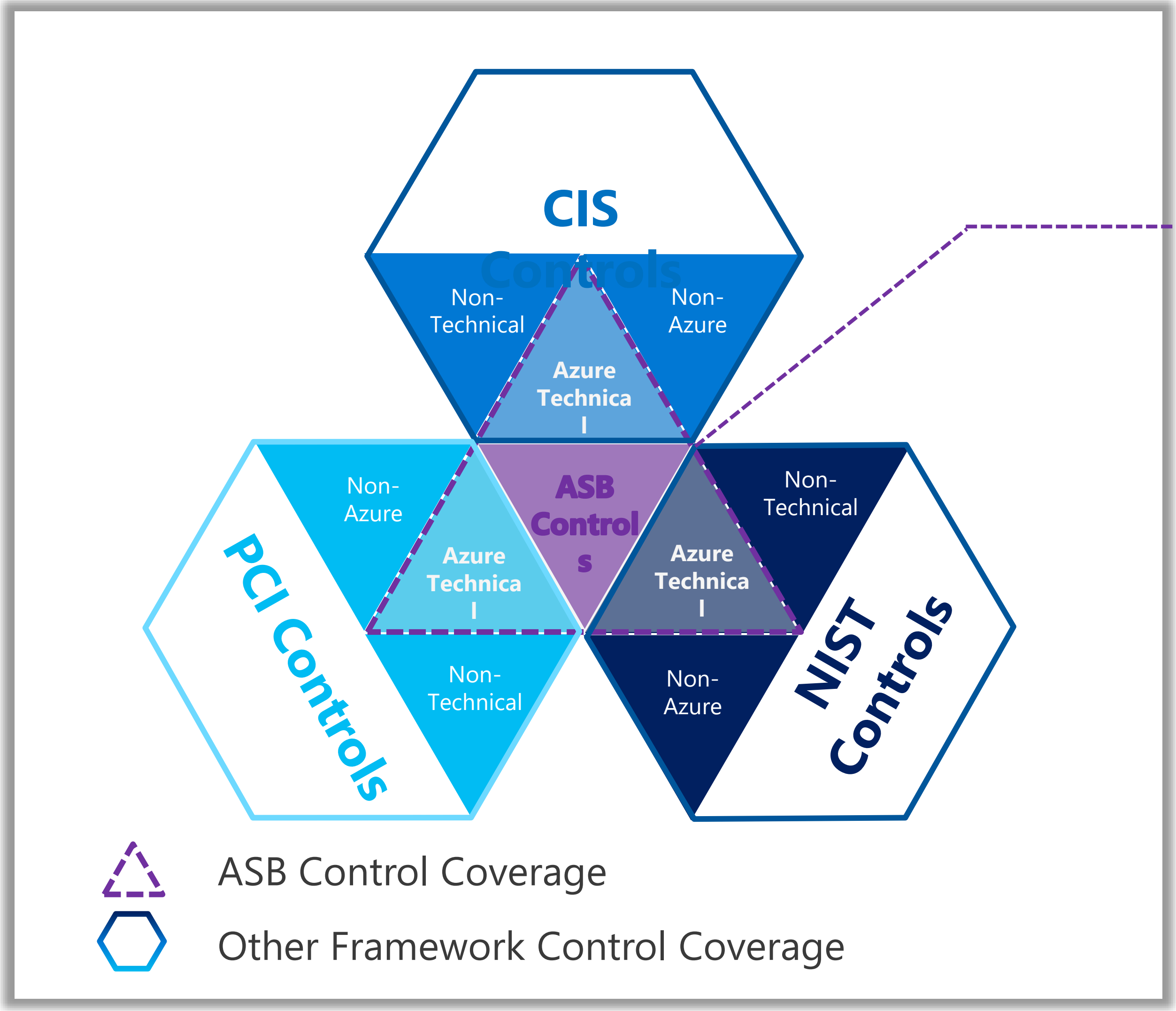
OVERVIEW

Azure Databricks

Azure Machine Learnings

Cognitive Services

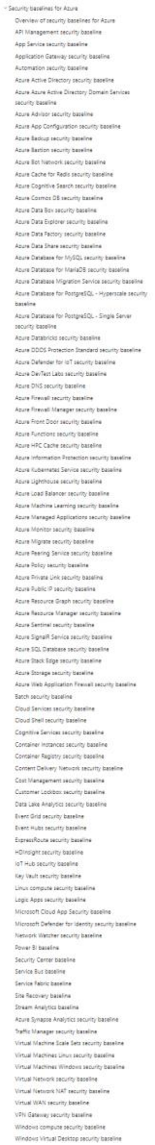
Current Azure Security Benchmark scope



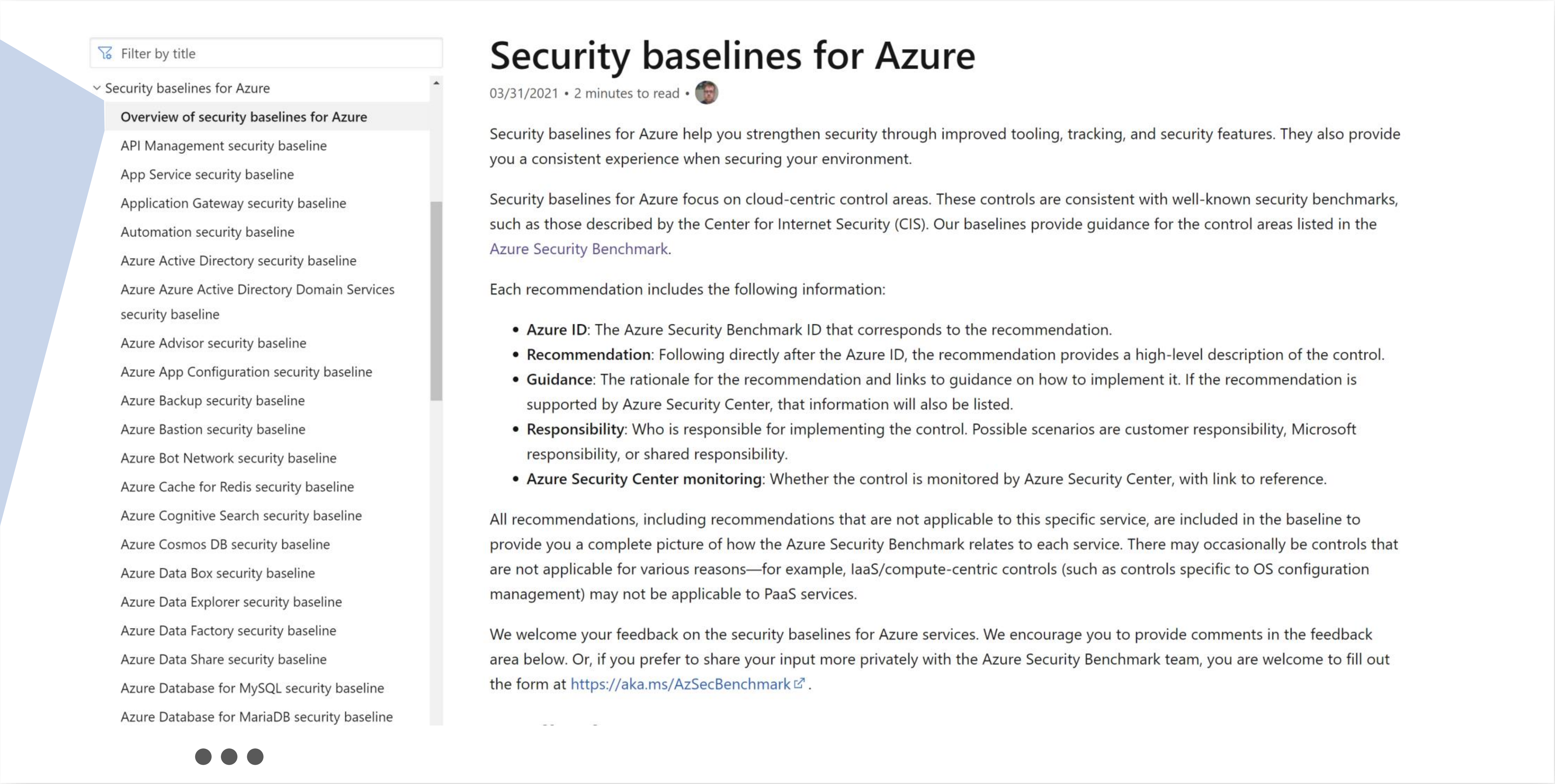
ASB provides a canonical set of **Azure-centric technical security controls** based on widely used security/compliance control frameworks such as CIS, NIST and PCI.

Baselines - Azure Security Benchmark

- Apply Azure Security Benchmark to Azure Services



- Security baselines for Azure
  - Overview of security baselines for Azure
  - API Management security baseline
  - App Service security baseline
  - Application Gateway security baseline
  - Automation security baseline
  - Azure Active Directory security baseline
  - Azure Azure Active Directory Domain Services security baseline
  - Azure Advisor security baseline
  - Azure App Configuration security baseline
  - Azure Backup security baseline
  - Azure Bastion security baseline
  - Azure Bot Network security baseline
  - Azure Cache for Redis security baseline
  - Azure Cognitive Search security baseline
  - Azure Cosmos DB security baseline
  - Azure Data Box security baseline
  - Azure Data Explorer security baseline
  - Azure Data Factory security baseline
  - Azure Data Share security baseline
  - Azure Database for MySQL security baseline
  - Azure Database for MariaDB security baseline
  - Azure Database Migration Service security baseline
  - Azure Database for PostgreSQL - Hyperscale security baseline
  - Azure Database for PostgreSQL - Single Server security baseline
  - Azure Databricks security baseline
  - Azure DDOS Protection Standard security baseline
  - Azure Defender for IoT security baseline
  - Azure DevTest Labs security baseline
  - Azure DNS security baseline
  - Azure Firewall security baseline
  - Azure Firewall Manager security baseline
  - Azure Front Door security baseline
  - Azure Functions security baseline
  - Azure HPC Cache security baseline
  - Azure Information Protection security baseline
  - Azure Kubernetes Service security baseline
  - Azure Lighthouse security baseline
  - Azure Load Balancer security baseline
  - Azure Machine Learning security baseline
  - Azure Managed Applications security baseline
  - Azure Monitor security baseline
  - Azure Migrate security baseline
  - Azure Peering Service security baseline
  - Azure Policy security baseline
  - Azure Private Link security baseline
  - Azure Public IP security baseline
  - Azure Resource Graph security baseline
  - Azure Resource Manager security baseline
  - Azure Sentinel security baseline
  - Azure SignalR Service security baseline
  - Azure SQL Database security baseline
  - Azure Stack Edge security baseline
  - Azure Storage security baseline
  - Azure Web Application Firewall security baseline
  - Batch security baseline
  - Cloud Services security baseline
  - Cloud Shell security baseline
  - Cognitive Services security baseline
  - Container Instances security baseline
  - Container Registry security baseline
  - Content Delivery Network security baseline
  - Cost Management security baseline
  - Customer Lockbox security baseline
  - Data Lake Analytics security baseline
  - Event Grid security baseline
  - Event Hubs security baseline
  - ExpressRoute security baseline
  - HDInsight security baseline
  - IoT Hub security baseline
  - Key Vault security baseline
  - Linux compute security baseline
  - Logic Apps security baseline
  - Microsoft Cloud App Security baseline
  - Microsoft Defender for Identity security baseline
  - Network Watcher security baseline
  - Power BI baseline
  - Security Center baseline
  - Service Bus baseline
  - Service Fabric baseline
  - Site Recovery baseline
  - Stream Analytics baseline
  - Azure Synapse Analytics security baseline
  - Traffic Manager security baseline
  - Virtual Machine Scale Sets security baseline
  - Virtual Machines Linux security baseline
  - Virtual Machines Windows security baseline
  - Virtual Network security baseline
  - Virtual Network NAT security baseline
  - Virtual WAN security baseline
  - VPN Gateway security baseline
  - Windows compute security baseline
  - Windows Virtual Desktop security baseline



- Security baselines for Azure
  - **Overview of security baselines for Azure**
  - API Management security baseline
  - App Service security baseline
  - Application Gateway security baseline
  - Automation security baseline
  - Azure Active Directory security baseline
  - Azure Azure Active Directory Domain Services security baseline
  - Azure Advisor security baseline
  - Azure App Configuration security baseline
  - Azure Backup security baseline
  - Azure Bastion security baseline
  - Azure Bot Network security baseline
  - Azure Cache for Redis security baseline
  - Azure Cognitive Search security baseline
  - Azure Cosmos DB security baseline
  - Azure Data Box security baseline
  - Azure Data Explorer security baseline
  - Azure Data Factory security baseline
  - Azure Data Share security baseline
  - Azure Database for MySQL security baseline
  - Azure Database for MariaDB security baseline

●●●

Security baselines for Azure

03/31/2021 • 2 minutes to read •

Security baselines for Azure help you strengthen security through improved tooling, tracking, and security features. They also provide you a consistent experience when securing your environment.

Security baselines for Azure focus on cloud-centric control areas. These controls are consistent with well-known security benchmarks, such as those described by the Center for Internet Security (CIS). Our baselines provide guidance for the control areas listed in the Azure Security Benchmark.

Each recommendation includes the following information:

- **Azure ID**: The Azure Security Benchmark ID that corresponds to the recommendation.
- **Recommendation**: Following directly after the Azure ID, the recommendation provides a high-level description of the control.
- **Guidance**: The rationale for the recommendation and links to guidance on how to implement it. If the recommendation is supported by Azure Security Center, that information will also be listed.
- **Responsibility**: Who is responsible for implementing the control. Possible scenarios are customer responsibility, Microsoft responsibility, or shared responsibility.
- **Azure Security Center monitoring**: Whether the control is monitored by Azure Security Center, with link to reference.

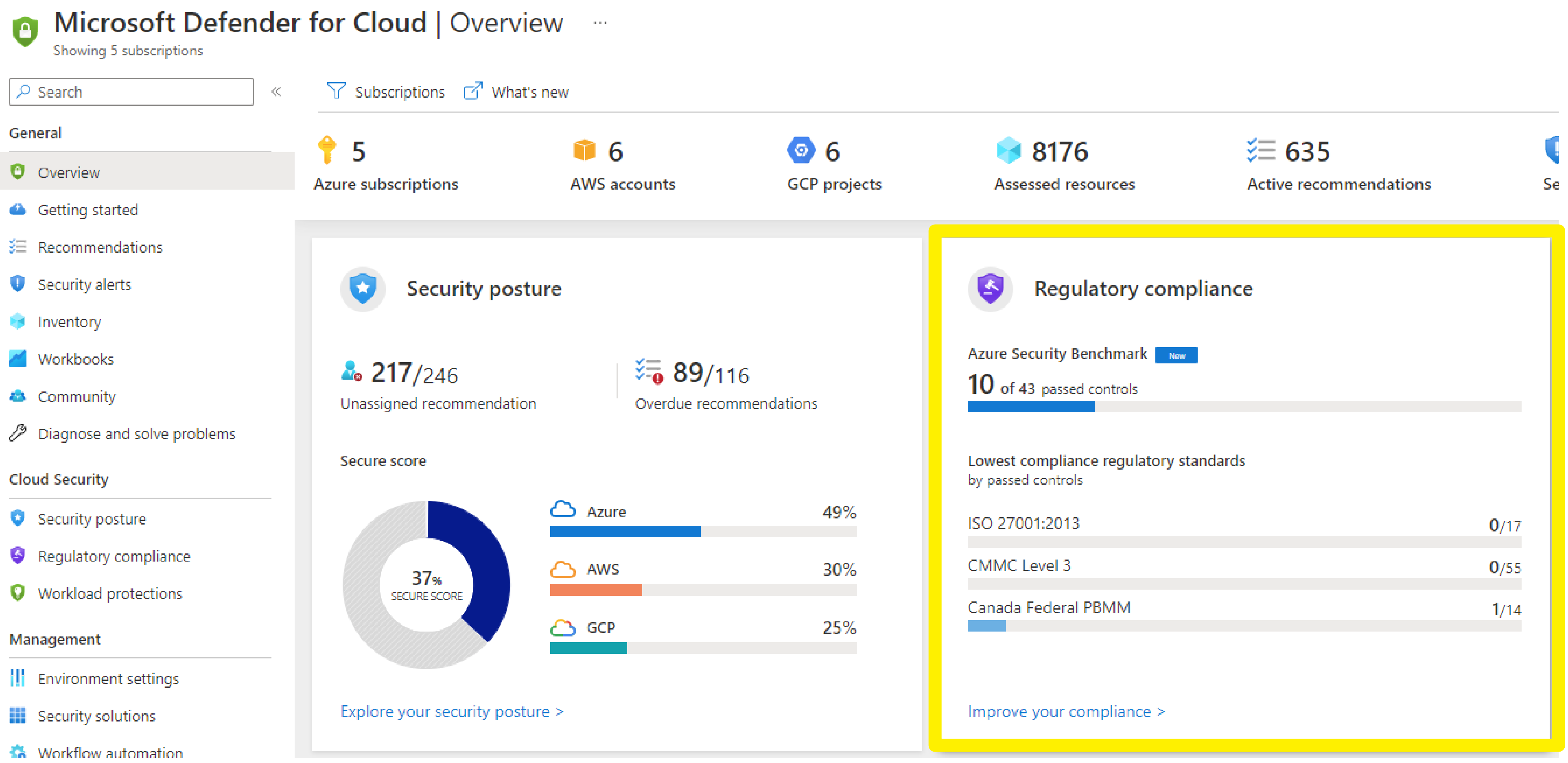
All recommendations, including recommendations that are not applicable to this specific service, are included in the baseline to provide you a complete picture of how the Azure Security Benchmark relates to each service. There may occasionally be controls that are not applicable for various reasons—for example, IaaS/compute-centric controls (such as controls specific to OS configuration management) may not be applicable to PaaS services.

We welcome your feedback on the security baselines for Azure services. We encourage you to provide comments in the feedback area below. Or, if you prefer to share your input more privately with the Azure Security Benchmark team, you are welcome to fill out the form at https://aka.ms/AzSecBenchmark .

Demo

Regulatory Compliance

Regulatory Compliance



Microsoft Defender for Cloud | Overview ...

Showing 5 subscriptions

Search

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections

Management

- Environment settings
- Security solutions
- Workflow automation

Subscriptions | What's new

5 Azure subscriptions | 6 AWS accounts | 6 GCP projects | 8176 Assessed resources | 635 Active recommendations | Se

Security posture

217/246 Unassigned recommendation

89/116 Overdue recommendations

Secure score

37% SECURE SCORE

Azure	49%
AWS	30%
GCP	25%

Explore your security posture >

Regulatory compliance

Azure Security Benchmark New

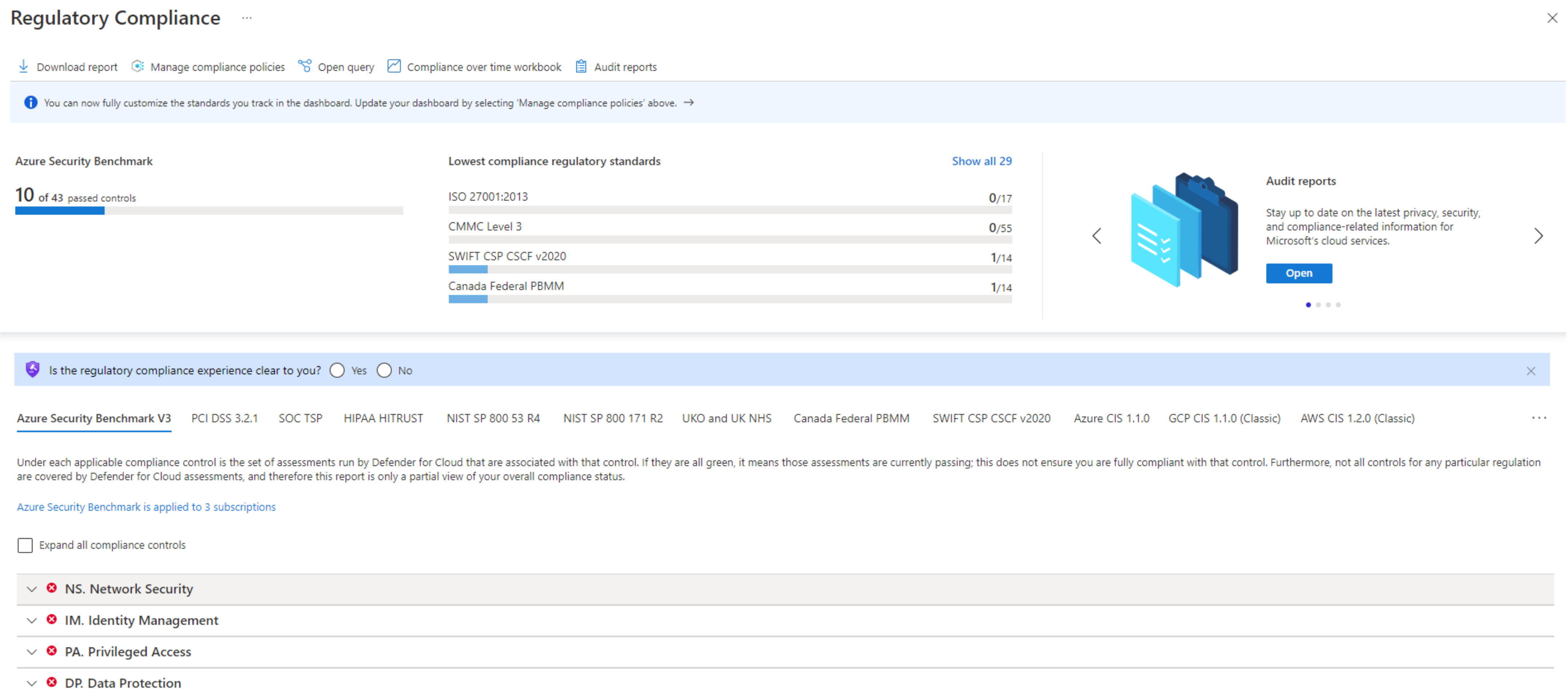
10 of 43 passed controls

Lowest compliance regulatory standards
by passed controls

ISO 27001:2013	0/17
CMMC Level 3	0/55
Canada Federal PBMM	1/14

Improve your compliance >

Regulatory Compliance



Regulatory Compliance ···

Download report · Manage compliance policies · Open query · Compliance over time workbook · Audit reports

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above. →

Azure Security Benchmark

10 of 43 passed controls

Lowest compliance regulatory standards

Show all 29

ISO 27001:2013	0/17
CMMC Level 3	0/55
SWIFT CSP CSCF v2020	1/14
Canada Federal PBMM	1/14

Audit reports

Stay up to date on the latest privacy, security, and compliance-related information for Microsoft's cloud services.

Open

Is the regulatory compliance experience clear to you? ○ Yes ○ No

Azure Security Benchmark V3 · PCI DSS 3.2.1 · SOC TSP · HIPAA HITRUST · NIST SP 800 53 R4 · NIST SP 800 171 R2 · UKO and UK NHS · Canada Federal PBMM · SWIFT CSP CSCF v2020 · Azure CIS 1.1.0 · GCP CIS 1.1.0 (Classic) · AWS CIS 1.2.0 (Classic) ···

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to 3 subscriptions

□ Expand all compliance controls

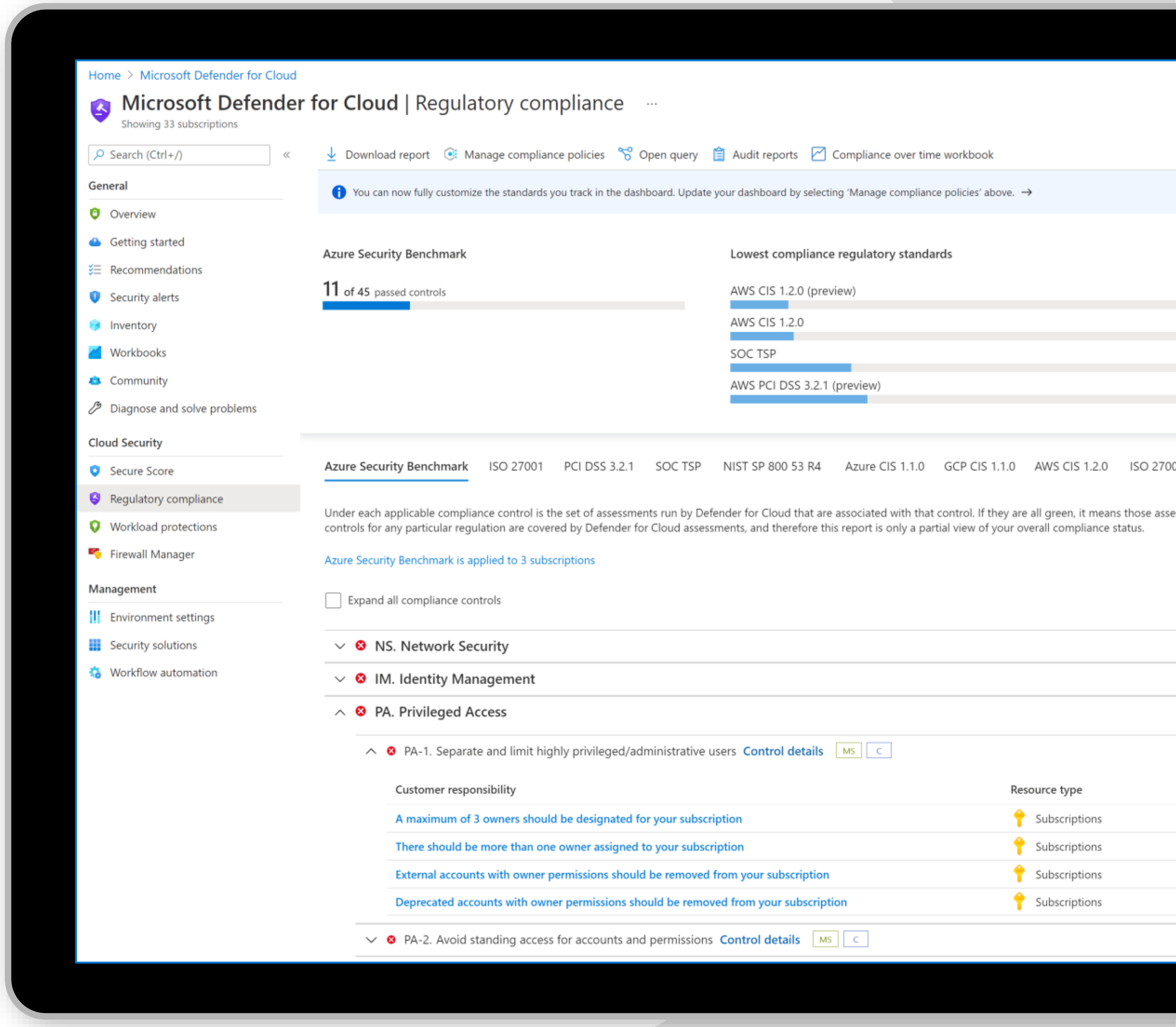
- NS. Network Security
- IM. Identity Management
- PA. Privileged Access
- DP. Data Protection

Compliance assessment and management

- → Assess and manage your compliance status with a continuous assessment of your cloud resources
- → Use industry standards, regulatory compliance frameworks, and vendor provided benchmarks to implement security and compliance best practices
- → Create custom recommendations to meet unique organizational needs

<u>Support for:</u>

- ✓ CIS
- ✓ PCI
- ✓ NIST
- ✓ SOC
- ✓ ISO
- ✓ HIPAA
- ✓ Local/National compliance standards
- ✓ Azure Security Benchmark
- ✓ AWS Foundational Security best practices



Microsoft Defender for Cloud | Regulatory compliance ···

Showing 33 subscriptions

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above. →

Azure Security Benchmark

11 of 45 passed controls

Lowest compliance regulatory standards

- AWS CIS 1.2.0 (preview)
- AWS CIS 1.2.0
- SOC TSP
- AWS PCI DSS 3.2.1 (preview)

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those asse controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to 3 subscriptions

☐ Expand all compliance controls

- ⊗ NS. Network Security
- ⊗ IM. Identity Management
- ⊗ PA. Privileged Access
  - ⊗ PA-1. Separate and limit highly privileged/administrative users Control details MS C

Customer responsibility	Resource type
A maximum of 3 owners should be designated for your subscription	Subscriptions
There should be more than one owner assigned to your subscription	Subscriptions
External accounts with owner permissions should be removed from your subscription	Subscriptions
Deprecated accounts with owner permissions should be removed from your subscription	Subscriptions

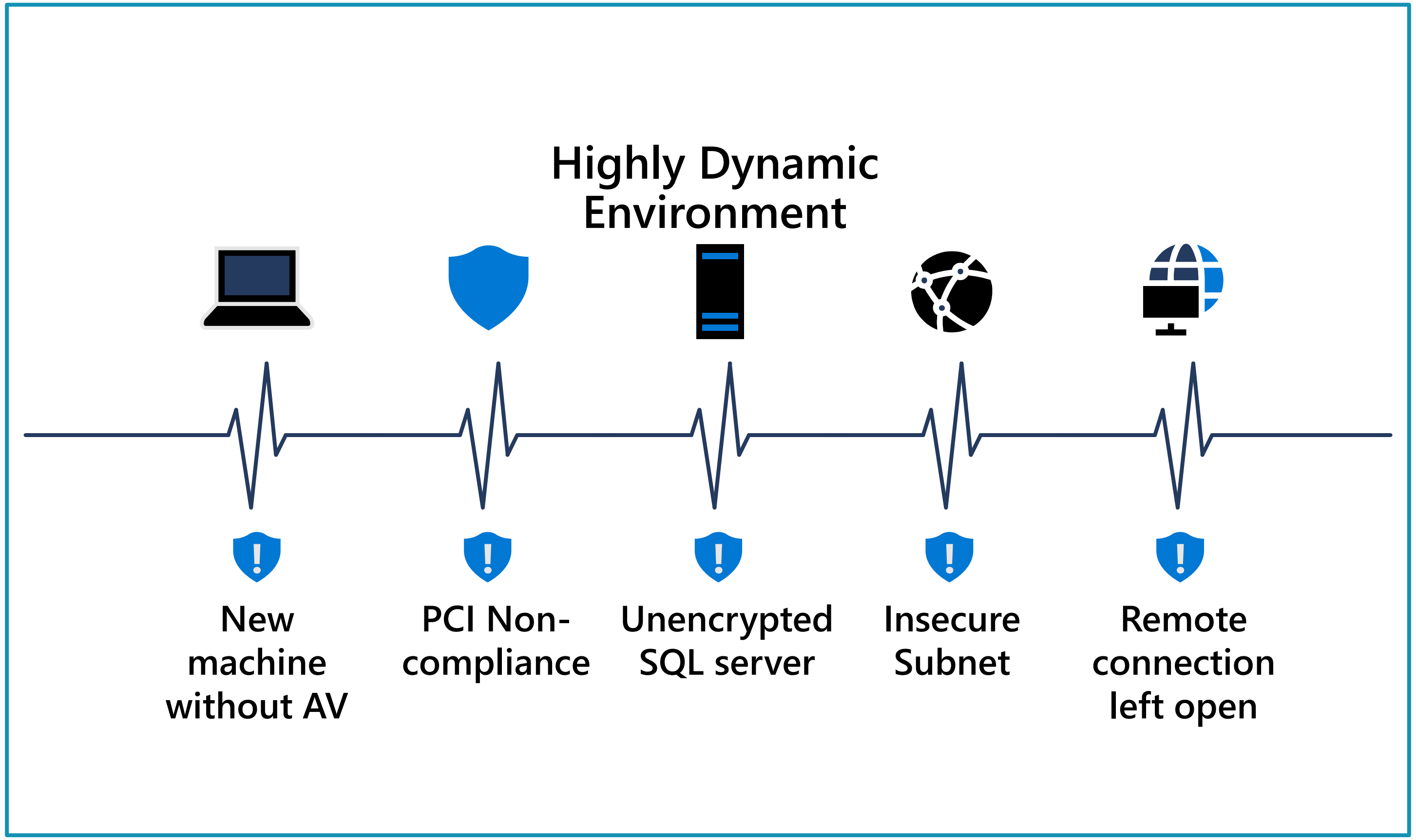
  - ⊗ PA-2. Avoid standing access for accounts and permissions Control details MS C

Manage organizational security policies and assess compliance in minutes

Manage security policies at an organizational level

Easily set security policies for subscriptions or management groups

Instantly understand your current policy compliance and review compliance overtime

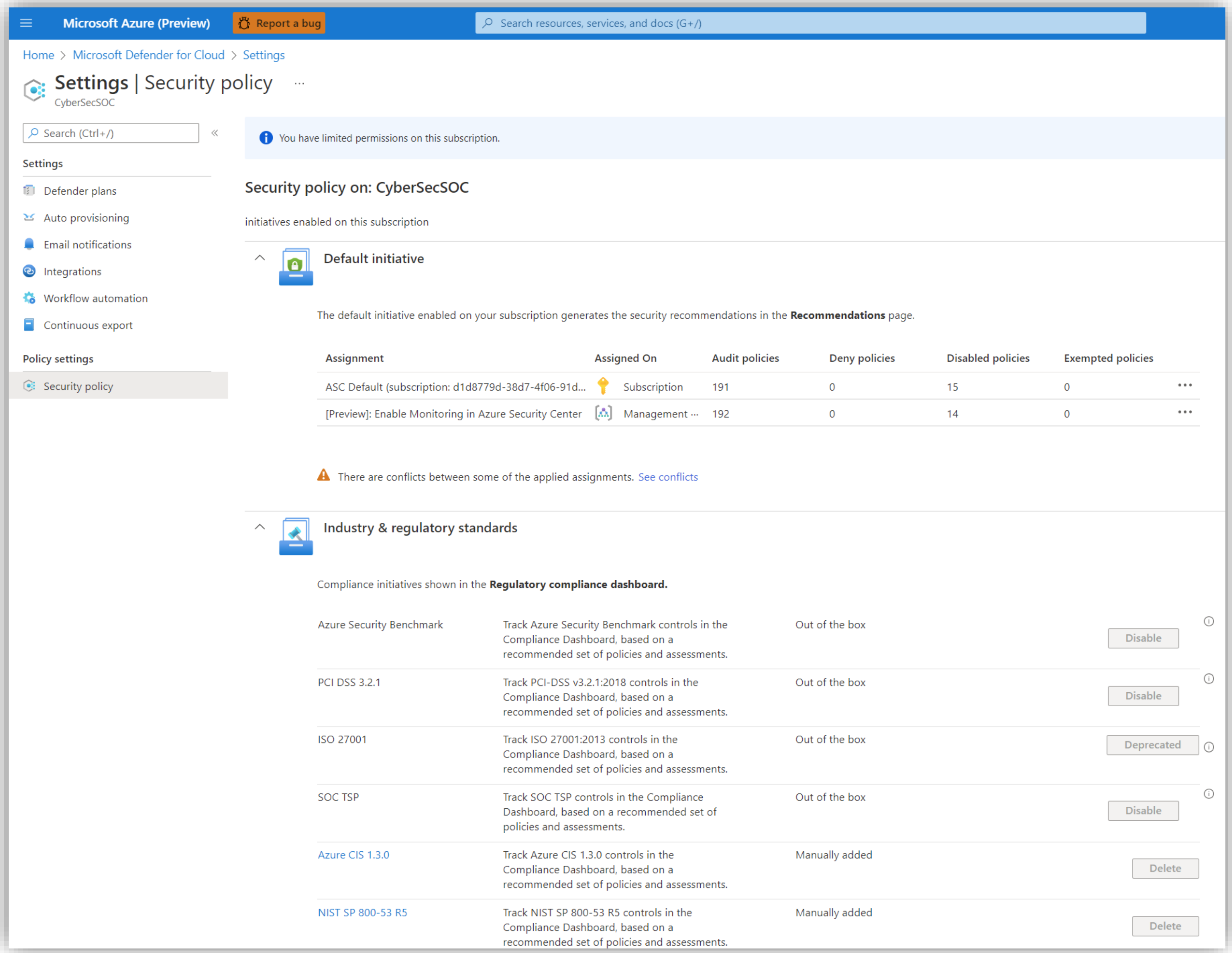


Editing security policies

You can edit security policies through the Azure Policy portal, via REST API or using Windows PowerShell

There are two specific roles

- Security reader
- Security admin



Settings | Security policy

CyberSecSOC

You have limited permissions on this subscription.

Security policy on: CyberSecSOC

initiatives enabled on this subscription

Default initiative

The default initiative enabled on your subscription generates the security recommendations in the **Recommendations** page.

Assignment	Assigned On	Audit policies	Deny policies	Disabled policies	Exempted policies
ASC Default (subscription: d1d8779d-38d7-4f06-91d...	Subscription	191	0	15	0
[Preview]: Enable Monitoring in Azure Security Center	Management ···	192	0	14	0

There are conflicts between some of the applied assignments. See conflicts

Industry & regulatory standards

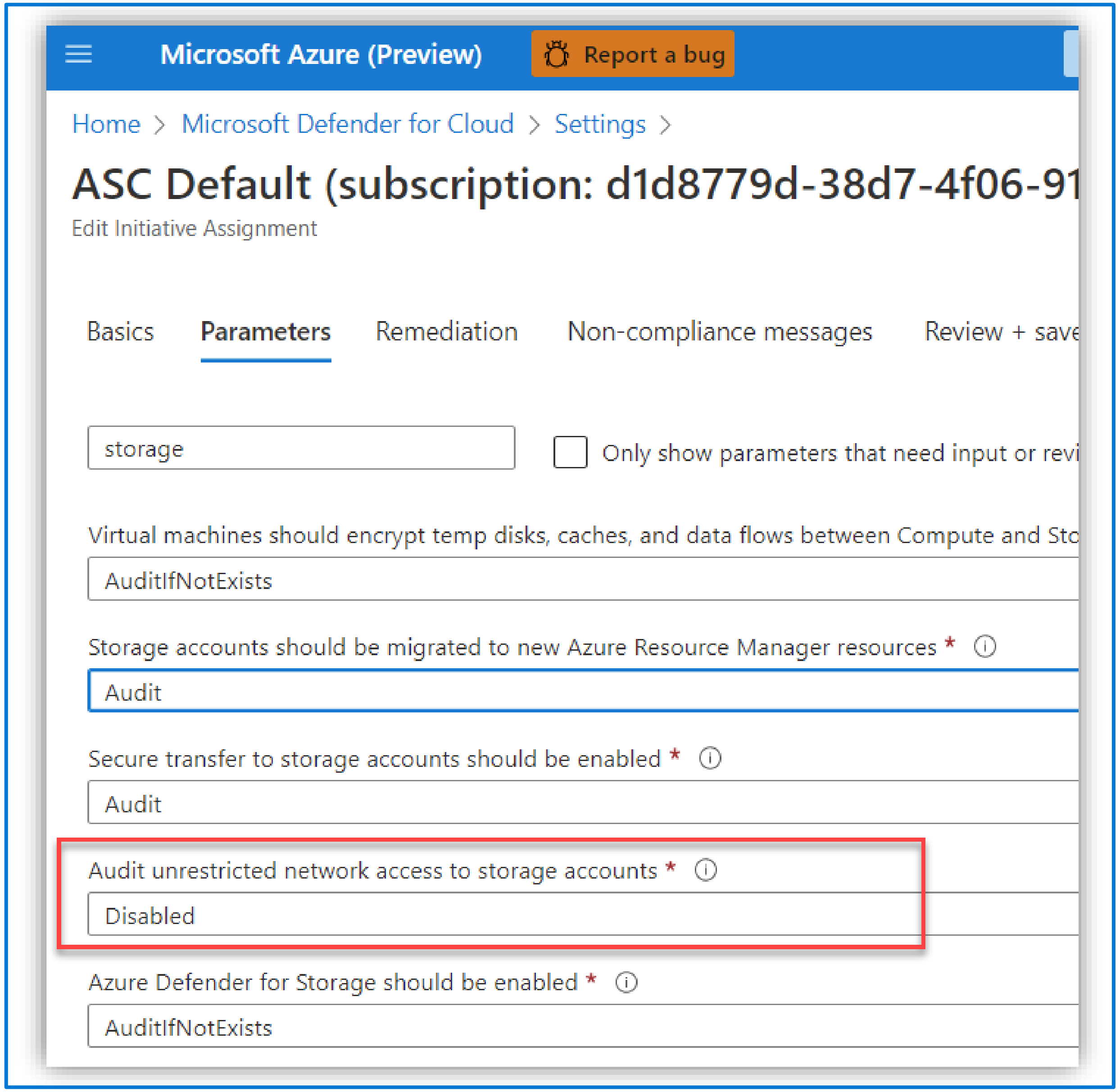
Compliance initiatives shown in the **Regulatory compliance dashboard.**

Azure Security Benchmark	Track Azure Security Benchmark controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Disable
PCI DSS 3.2.1	Track PCI-DSS v3.2.1:2018 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Disable
ISO 27001	Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Deprecated
SOC TSP	Track SOC TSP controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Disable
Azure CIS 1.3.0	Track Azure CIS 1.3.0 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Manually added	Delete
NIST SP 800-53 R5	Track NIST SP 800-53 R5 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Manually added	Delete

Disabling security policies and recommendations

When your security initiative triggers a recommendation that's irrelevant for your environment, you can prevent that recommendation from appearing again

To disable a recommendation, disable the specific policy that generates the recommendation



Home > Microsoft Defender for Cloud > Settings >

ASC Default (subscription: d1d8779d-38d7-4f06-91

Edit Initiative Assignment

storage

□ Only show parameters that need input or revi

Virtual machines should encrypt temp disks, caches, and data flows between Compute and Sto

AuditIfNotExists

Storage accounts should be migrated to new Azure Resource Manager resources *

Audit

Secure transfer to storage accounts should be enabled *

Audit

Audit unrestricted network access to storage accounts *

Disabled

Azure Defender for Storage should be enabled *

AuditIfNotExists

Demo - Regulatory Compliance

Azure Policy

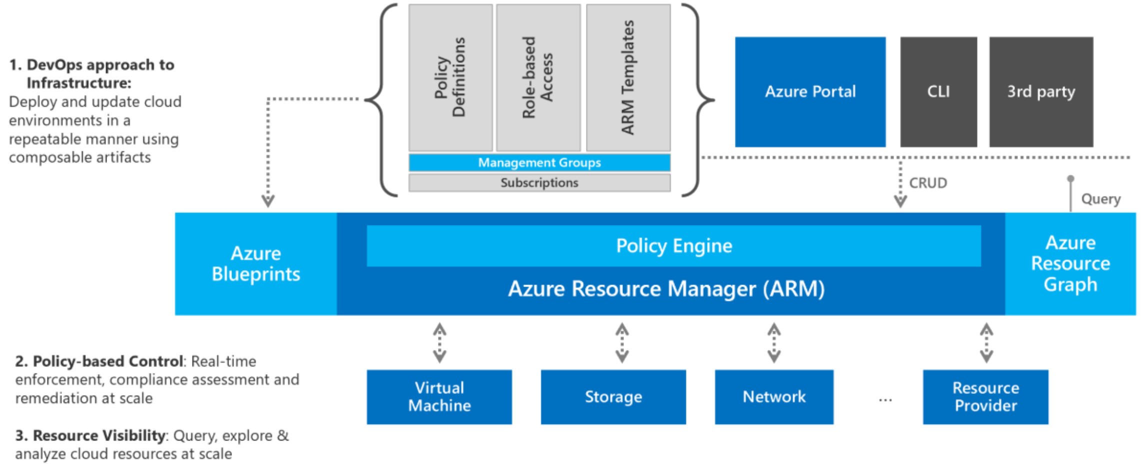
Overview

Azure Policy helps to enforce organizational standards and to 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 the per-resource, per-policy granularity. It also helps to bring your resources to compliance through bulk remediation for existing resources and automatic remediation for new resources.

Documentation Link

- [Overview of Azure Policy - Azure Policy | Microsoft Docs]()

Azure Governance Architecture



1. DevOps approach to Infrastructure: Deploy and update cloud environments in a repeatable manner using composable artifacts

2. Policy-based Control: Real-time enforcement, compliance assessment and remediation at scale

3. Resource Visibility: Query, explore & analyze cloud resources at scale

Regulatory Compliance built-ins

https://learn.microsoft.com/en-us/azure/governance/policy/samples/azure-security-benchmark

- Azure Security Benchmark
- CIS Benchmark 1.3.0
- CIS Benchmark 1.1.0
- CMMC Level 3
- FedRAMP Moderate
- FedRAMP High
- HIPAA HITRUST 9.2
- IRS 1075 September 2016
- ISO 27001:2013
- PCI DSS 3.2.1

Regulatory Compliance built-ins

https://learn.microsoft.com/en-us/azure/governance/policy/samples/azure-security-benchmark

- NIST SP800-53 Rev. 5
- NIST SP 800-53 Rev.4
- NIST SP 800-171 R2
- RBI ITF NBFC v2017
- SWIFT CSCF 2021
- Canada Federal PBMM
- RMIT Malaysia
- New Zealand ISM Redistricted v3.5
- UK OFFICIAL and UK NHS

Regulatory Compliance built-ins (Azure Government)

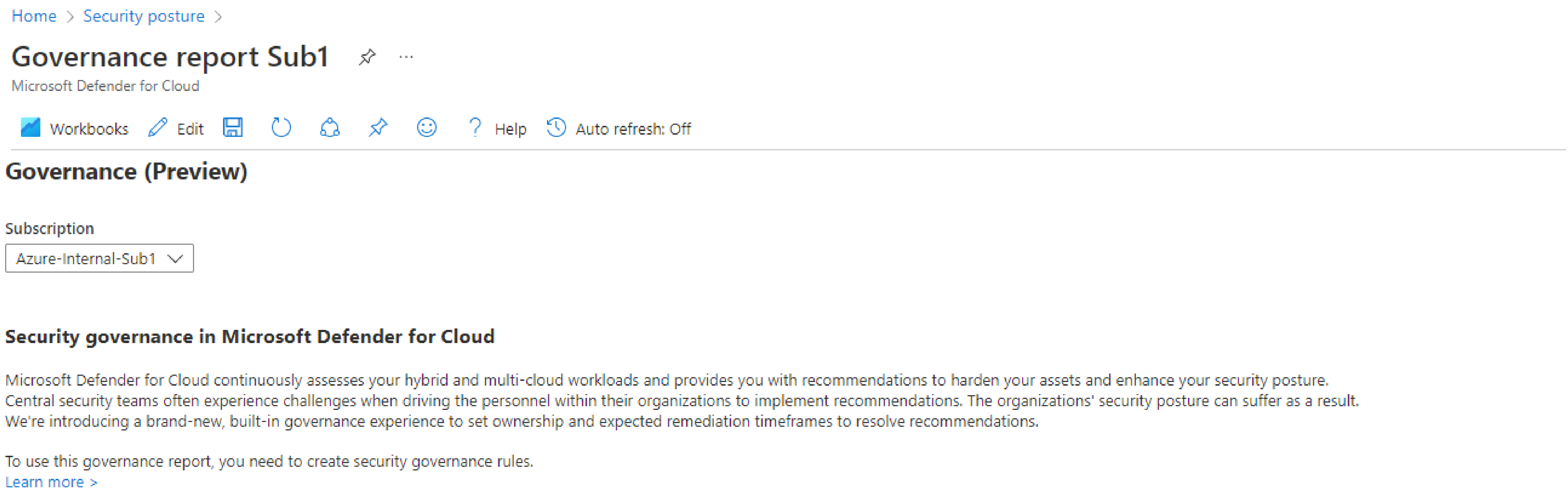
https://learn.microsoft.com/en-us/azure/governance/policy/samples/gov-azure-security-benchmark

- Azure Security Benchmark
- CIS Benchmark 1.3.0
- CIS Benchmark 1.1.0
- CMMC Level 3
- DoD Impact Level 4
- DoD Impact Level 5
- FedRAMP Moderate
- FedRAMP High
- IRS 1075 September 2016
- ISO 27001:2013
- NIST SP 800-53 Rev. 5
- NIST SP 800-53 Rev. 4
- NIST SP 800-171 R2

Demo - Azure Policy

Governance Workbooks and Rules (Preview)

Security teams who do not have ability to implement security recommendations can assign owners with due dates to recommendations using Governance rules.



Governance report Sub1

Microsoft Defender for Cloud

Governance (Preview)

Subscription

Azure-Internal-Sub1

Security governance in Microsoft Defender for Cloud

Microsoft Defender for Cloud continuously assesses your hybrid and multi-cloud workloads and provides you with recommendations to harden your assets and enhance your security posture. Central security teams often experience challenges when driving the personnel within their organizations to implement recommendations. The organizations' security posture can suffer as a result. We're introducing a brand-new, built-in governance experience to set ownership and expected remediation timeframes to resolve recommendations.

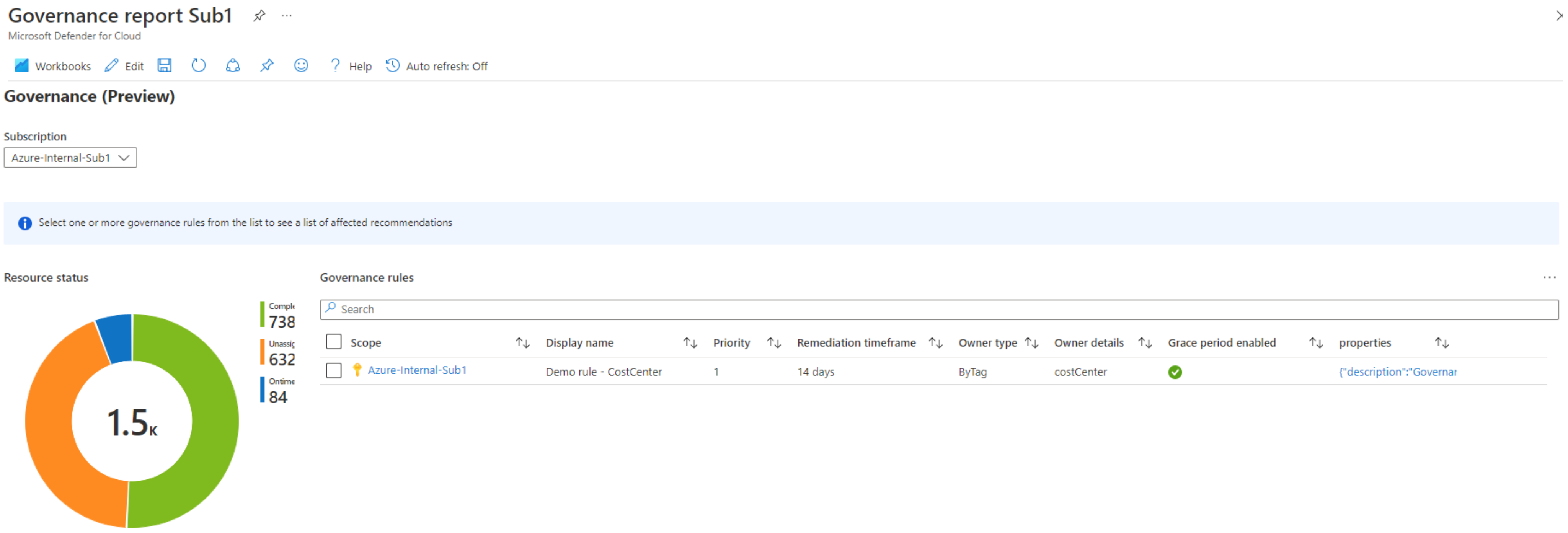
To use this governance report, you need to create security governance rules.

Learn more >

[Driving your organization to remediate security issues with recommendation governance in Microsoft Defender for Cloud | Microsoft Learn]

Governance Workbooks and Rules (Preview)

Governance Workbooks can track rules, ownership, recommendations and remediation status.



Governance report Sub1

Microsoft Defender for Cloud

Governance (Preview)

Subscription: Azure-Internal-Sub1

Select one or more governance rules from the list to see a list of affected recommendations

Governance rules

□	Scope	Display name	Priority	Remediation timeframe	Owner type	Owner details	Grace period enabled	properties
□	Azure-Internal-Sub1	Demo rule - CostCenter	1	14 days	ByTag	costCenter	✓	{"description":"Governar

©Microsoft Corporation
Azure

Demo of Governance (Preview)

Wrap-up

Resources

MDC
https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-cloud-introduction
Security policies, initiatives and recommendations
https://learn.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept
Azure recommendations
https://learn.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference
AWS recommendations
https://learn.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference-aws

Microsoft Defender for Cloud

- Secure and protect resources across the three major cloud providers and hybrid environments in one place
- Ensure secure and compliant configuration of cloud resources
- Detect vulnerabilities and threats to protect against malicious attacks

Microsoft Azure

aws

Strengthen you cloud security posture today

Enable Defender for Cloud to assess your security posture

Fix your top 5 Secure Score recommendations today

Start a free trial to protect your workloads

Onboard AWS, GCP and on-prem workloads with Azure Arc

To learn more, visit: aka.ms/DefenderForCloud >>

Microsoft Security

Thank you