CIS Microsoft Azure Foundations Benchmark

v3.0.0 - 09-05-2024

Terms of Use

Please see the below link for our current terms of use:

https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/

For information on referencing and/or citing CIS Benchmarks in 3rd party documentation (including using portions of Benchmark Recommendations) please contact CIS Legal (CISLegal@cisecurity.org) and request guidance on copyright usage.

NOTE: It is ***NEVER*** acceptable to host a CIS Benchmark in ***ANY*** format (PDF, etc.) on a 3rd party (non-CIS owned) site.

Table of Contents

Overview

All CIS Benchmarks™ focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system and applications for vulnerabilities and quickly updating with the latest security patches.
- End-point protection (Antivirus software, Endpoint Detection and Response (EDR), etc.).
- Logging and monitoring user and system activity.

In the end, the CIS Benchmarks™ are designed to be a key **component** of a comprehensive cybersecurity program.

Important Usage Information

All CIS Benchmarks™ are available free for non-commercial use from the CIS Website. They can be used to ***manually*** assess and remediate systems and applications. In lieu of manual assessment and remediation, there are several tools available to assist with assessment:

- CIS Configuration Assessment Tool (CIS-CAT® Pro Assessor)
- CIS Benchmarks™ Certified 3rd Party Tooling

These tools make the hardening process much more scalable for large numbers of systems and applications.

> **NOTE**: Some tooling focuses only on the CIS Benchmarks™ Recommendations that can be fully automated (skipping ones marked **Manual**). It is important that ***ALL*** Recommendations (**Automated** and **Manual**) be addressed, since all are important for properly securing systems and are typically in scope for audits.

In addition, CIS has developed CIS Build Kits for some common technologies to assist in applying CIS Benchmarks™ Recommendations.

When remediating systems (changing configuration settings on deployed systems as per the CIS Benchmarks™ Recommendations), please approach this with caution and test thoroughly.

The following is a reasonable remediation approach to follow:

1. **NEVER** deploy a CIS Build Kit, or any internally developed remediation method, to production systems without proper testing.
2. Proper testing consists of the following:

a. Understand the configuration (including installed applications) of the targeted systems.

b. Read the Impact section of the given Recommendation to help determine if there might be an issue with the targeted systems.

c. Test the configuration changes on representative lab system(s). This way if there is some issue it can be resolved prior to deploying to any production systems.

d. When confident, initially deploy to a small sub-set of users and monitor closely for issues. This way if there is some issue it can be resolved prior to deploying more broadly.

e. When confident, iteratively deploy to additional groups and monitor closely for issues until deployment is complete. This way if there is some issue it can be resolved prior to continuing deployment.

NOTE: CIS and the CIS Benchmarks™ development communities in CIS WorkBench do their best to test and have high confidence in the Recommendations, but they cannot test potential conflicts with all possible system deployments. Known potential issues identified during CIS Benchmarks™ development are documented in the Impact section of each Recommendation.

By using CIS and/or CIS Benchmarks™ Certified tools, and being careful with remediation deployment, it is possible to harden large numbers of deployed systems in a cost effective, efficient, and safe manner.

NOTE: As previously stated, the PDF versions of the CIS Benchmarks™ are available for free, non-commercial use on the CIS Website. All other formats of the CIS Benchmarks™ (MS Word, Excel, and Build Kits) are available for CIS SecureSuite® members.

CIS-CAT® Pro is also available to CIS SecureSuite® members.

Target Technology Details

This document, CIS Microsoft Azure Foundations Benchmark, provides prescriptive guidance for establishing a secure baseline configuration for Microsoft Azure. The scope of this benchmark is to establish the foundation level of security for anyone adopting Microsoft Azure cloud services. The benchmark is, however, not an exhaustive list of all possible security configurations and architecture. The benchmark should be understood as a starting point. Site-specific tailoring will almost certainly be required. The CIS Azure Foundations Benchmark provides recommendations for a variety of Microsoft Azure Services including the following:

- Microsoft Entra ID (Azure Active Directory)
- Microsoft Defender for Cloud
- Microsoft Azure App Service
- Microsoft Azure Database Services

- Microsoft Azure Storage Accounts
- Microsoft Azure Monitor
- Microsoft Azure Networking
- Microsoft Azure Virtual Machines

To obtain the latest version of this guide, please visit https://benchmarks.cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at BenchmarkInfo@cisecurity.org.

Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Azure.

Consensus Guidance

This CIS Benchmark™ was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit https://workbench.cisecurity.org/.

Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, UI/Menu selections or examples. Text should be interpreted exactly as presented.
`<Monospace font in brackets>`	Text set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to reference other relevant settings, CIS Benchmarks and/or Benchmark Communities. Also, used to denote the title of a book, article, or other publication.
Bold font	Additional information or caveats things like **Notes**, **Warnings**, or **Cautions** (usually just the word itself and the rest of the text normal).

Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

Title

Concise description for the recommendation's intended configuration.

Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

Impact Statement

Any security, functionality, or operational consequences that can result from following the recommendation.

Audit Procedure

Systematic instructions for determining if the target system complies with the recommendation.

Remediation Procedure

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

Default Value

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

References

Additional documentation relative to the recommendation.

CIS Critical Security Controls® (CIS Controls®)

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) “5.1 - Establish Secure Configurations” and (v8) '4.1 - Establish and Maintain a Secure Configuration Process” so individual recommendations will not be mapped to these safeguards.

Additional Information

Supplementary information that does not correspond to any other field but may be useful to the user.

Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

  Items in this profile intend to:

  - be practical and prudent;
  - provide security focused best practice hardening of a technology; and
  - limit impact to the utility of the technology beyond acceptable means.

- **Level 2**

  This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

  - are intended for environments or use cases where security is more critical than manageability and usability
  - acts as defense in depth measure
  - may impact the utility or performance of the technology
  - may include additional licensing, cost, or addition of third party software

Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Contributor
Zeeshan Mustafa
Logan McMillan
Jim Cheng
Stephen Keller
Jonathan Trull
Pravin Goyal
Prabhu Angadi
Robin Drake
Rahul Khengare
Mike Wicks
Clifford Moten
Ronit Reger
Lewis Hardy
Gareth Boyes
Ellie Goggin
Sagar Chhatrala
Jeffrey Lemmermann
Richard Rives
Nirbhay Kumar
Bhushan Bhat
Jordan Pitcairn
Harshal Khachane
Pavol Ilko
Karan Ahuja
Rahul Pareek
Luke Schultheis

Editor
Rachel Rice
Ian McRee
Robert Burton
Zan Liffick
Iben Rodriguez
Michael Born
Niclas Madsen
Steve Johnson

Recommendations

1 Introduction

This introduction section and the subsections herein provide informative articles which instruct on the use of the CIS Foundations and Service Category Benchmarks. No recommendations will be found in this section, just articles of relevant information.

Please carefully review the articles in this introductory section and orient yourself with our structured approach to Benchmarking for Cloud Service Providers (CSPs). This approach differs from other CIS Benchmarks because:

- there are too many different products/services in CSP product directories to practically cover in any one Benchmark,
- architectural and design decisions will affect the scope and relevance of recommendations, and
- there are a variety of methods for interfacing with CSP products and services.

Cloud Benchmarks - A Two-Step Approach to Securing Your Cloud Environments:

- **Step 1:** Start with Foundations Benchmarks. Apply as many recommendations as **practical** for your environment; "100%" 'compliance' is not always possible. Not all Foundations Benchmark recommendations can be applied at the same time, and not all recommendations will be relevant to your environment. Use the recommendation Profile Levels and your understanding of your unique environment architecture to determine which recommendations are in scope.
- **Step 2:** Use the Service Category Benchmarks for service-specific defense-in-depth recommendations. Apply recommendations only for the services **IN USE** in your environment. Use the recommendation Profile Levels, and your understanding of your unique environment architecture to determine which recommendations are in scope.

1.1 CIS Microsoft Azure Foundations Benchmarks

The suggested approach for securing your Microsoft Azure cloud environment is to start with the **latest version** of the CIS Microsoft Azure Foundations Benchmark. Because CSP environments are constantly changing, previous versions of the Foundations Benchmarks should not be used; they are very likely to contain incorrect product names, outdated procedures, deprecated features, and other inaccuracies. The CIS Foundations Benchmark provides prescriptive guidance for configuring a subset of Microsoft Azure Services with an emphasis on foundational, testable, and architecture agnostic settings for services.

The Microsoft Azure Foundation Benchmark is what you should start with when beginning to secure your Azure environment. It is also the foundation for which all other Azure Service Category Benchmarks are built on so that as you grow your cloud presence and usage of the services offered you have the necessary guidance to securely configure your environment as it fits with your company's policy.

All CIS Benchmarks are created and maintained through consensus-based collaboration. Should you have feedback, suggested changes, or just like to get involved in the continued maintenance and development of CIS Microsoft Azure Benchmarks, please register on CIS WorkBench at https://workbench.cisecurity.org and join the CIS Microsoft Azure Benchmarks Community.

1.2 CIS Microsoft Azure Service Category Benchmarks

After configuring your environment with the CIS Microsoft Azure Foundations Benchmark, we suggest pursuing defense-in-depth and service-specific recommendations for your Azure Services by reviewing the Service Category Benchmarks. The Service Category Benchmarks are being produced with the vision that recommendations for all security-relevant products/services offered by a CSP should have a 'home,' but the Foundations Benchmarks should retain the most crucial recommendations and not be made vast, intimidating, and impractical.

The Service Category Benchmark recommendations should be applied **ONLY** for the CSP products and services that are actively **IN USE** in your environment. In each Service Category Benchmark, you may find that your environment uses none, or only a couple services from a list of many. Please review the services employed in your environment carefully to accurately scope the recommendations you apply. Failure to apply only the recommendations you need may introduce vulnerabilities, technical debt, and unnecessary expenses.

Using the Microsoft Azure Product Directory (https://azure.microsoft.com/en-us/products/) as a source of categorical grouping of these services, our vision is to produce a full set of CIS Microsoft Azure Service Category Benchmarks to cover all security-relevant services. A list of planned and published Service Category Benchmarks for the Azure Community can be found on the community dashboard here: https://workbench.cisecurity.org/communities/72.

Your help is needed to bring this vision to life! Please consider joining our CIS Microsoft Azure Community to contribute your expertise and knowledge in securing products and services from the Microsoft Azure product family.

All CIS Benchmarks are created and maintained through consensus-based collaboration. Should you have feedback, suggested changes, or just like to get involved in the continued maintenance and development of CIS Microsoft Azure Benchmarks, please register on CIS WorkBench at https://workbench.cisecurity.org and join the CIS Microsoft Azure Benchmarks community.

1.3 Multiple Methods of Audit and Remediation

Throughout the Benchmark, Audit and Remediation procedures are prescribed using up to five different methods. These multiple methods are presented for the convenience of readers who will be coming from different technical and experiential backgrounds. To perform any given Audit or Remediation, only one method needs to be performed. Not every method is available for every recommendation, and many that are available are not yet written for every recommendation. The methods presented in the Benchmark are formatted and titled as follows:

- "**From Azure Portal**" - This is the administrative GUI accessed at https://portal.azure.com.
- "**From Azure CLI**" - See additional detail in the next section.
- "**From PowerShell**" - See additional detail in the next section.
- "**From REST API**" - An Application Programming Interface (API) for HTTP operations on service endpoints.
- "**From Azure Policy**" - Azure Policy is administered from the Microsoft Defender for Cloud blade where Policy Initiatives can be created from "Regulatory Compliance" or by using pre-built Industry & Regulatory Standards.

Setting Up PowerShell and Azure CLI

In order to use the Azure Command Line Interface (CLI) and the Azure PowerShell methods for audit and remediation procedures, the following permissions are required for the account running the procedures:

1. Global Reader
2. Security Reader
3. Subscription Contributor
4. Key Vault Get/List privileges on Keys, Secrets, Certificates, and Certificate Authorities
5. Network allow listing for any source IP address performing the audit activities
6. Permissions to use PowerShell and Azure CLI

These permissions can be directly assigned or assigned via Privileged Identity Management.

The Azure CLI tool can be installed from the following location: https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows?tabs=azure-cli

For PowerShell, the following cmdlets are required:

1. Azure PowerShell: https://docs.microsoft.com/en-us/powershell/azure/install-az-ps-msi?view=azps-12.2.0
2. Microsoft Graph PowerShell: https://learn.microsoft.com/en-us/powershell/microsoftgraph/get-started?view=graph-powershell-1.0
3. Azure AD PowerShell for Graph: `[*Deprecation Planned]`

4. MS Online PowerShell: `[*Deprecation Planned]`

**Deprecation Planned*: Azure AD, Azure AD Preview and MSOnline PowerShell modules are planned for deprecation. Microsoft Graph PowerShell is the PowerShell module to use for interacting with Microsoft Entra ID and other Microsoft services. This reference of mapped cmdlets can help where replacement commands are needed: https://learn.microsoft.com/en-us/powershell/microsoftgraph/azuread-msoline-cmdlet-map?view=graph-powershell-1.0.

Authenticating with Azure CLI

Run the following command from either PowerShell or command prompt:

```
az login --tenant <tenant id> --subscription <subscription ID>
```

Authenticating with PowerShell

Login to the Azure tenant and subscription using the following command:

```
Connect-AzAccount -DeviceCode
```

1. Navigate a browser to https://microsoft.com/devicelogin
2. Enter the code returned from running the `Connect-AzAccount -DeviceCode` command above
3. When prompted, login with your Azure account credentials or if already authenticated, choose the correct Azure account.
4. If asked `Are you trying to sign into Azure PowerShell?`, click `Continue`.
5. Close the browser or browser tab when completed.

For the remaining PowerShell modules, the log in method is the same for now, though when logging into the `AzureAD` PowerShell module, you may get a warning to use the `MgGraph` PowerShell module instead. To log in to each, run the following commands.

```
Connect-MgGraph
Connect-AzureAD
```

NOTE: This may store session information within the PowerShell environment and may persist after closing PowerShell. Please take all necessary precautions to shorten the lifespan of this session and protect it from unauthorized access.

2 Identity

This section covers security best practice recommendations for products in the Azure Identity services category.

Azure Product Category Page: https://azure.microsoft.com/en-us/products/category/identity

Many of the recommendations from this section are marked as "Manual" while the existing Azure CLI and Azure AD PowerShell support through the Azure AD Graph are being deprecated. It is now recommended to use the new Microsoft Graph PowerShell in replacement of Azure AD Graph for PowerShell and API level access. From a security posture standpoint, these recommendations are still very important and should not be discounted because they are "Manual." As automation capability is developed for this Benchmark, the related recommendations will be updated with the respective audit and remediation steps and changed to an "automated" assessment status.

If any problems are encountered running Azure CLI or PowerShell methodologies, please refer to the Introduction section of this Benchmark where you will find additional detail on permission and required cmdlets.

2.1 Security Defaults (Per-User MFA)

IMPORTANT: READ BELOW BEFORE PROCEEDING!

- If your organization pays for Microsoft Entra ID licensing (included in Microsoft 365 E3, E5, or F5, and EM&S E3 or E5 licenses) and **CAN** use Conditional Access, ignore the recommendations in this section and proceed to the Conditional Access section.
- If your organization is using the free tier of Entra ID (Office 365 E1, E3, or E5, and Microsoft 365 F1 or F3 licenses) and **CAN NOT** use Conditional Access, proceed with the Security Defaults guidance in this section, and ignore the recommendations in the Conditional Access section.

Conditional Access is preferred, but Security Defaults (Per-User MFA) is recommended only if Conditional Access isn't available.

Why is this **IMPORTANT**?

The Azure "Security Defaults" recommendations represent an entry-level set of recommendations (such as Multi-Factor Authentication) which will be relevant to organizations and tenants that are either just starting to use Azure, or are only utilizing a bare minimum feature set, and rely on the free license tier of Microsoft Entra ID. Security Defaults recommendations are intended to ensure that these use cases are still capable of establishing a strong baseline of secure configuration.

If your subscription is licensed to use Microsoft Entra ID P1 or P2, it is strongly recommended that the "Security Defaults" section (this section and the recommendations therein) be bypassed in favor of the use of "Conditional Access."

IMPORTANT: READ ABOVE BEFORE PROCEEDING!

2.1.1 Ensure Security Defaults is enabled on Microsoft Entra ID (Manual)

Profile Applicability:

- Level 1

Description:

[**IMPORTANT - Please read the section overview:** If your organization pays for Microsoft Entra ID licensing (included in Microsoft 365 E3, E5, or F5, and EM&S E3 or E5 licenses) and **CAN** use Conditional Access, ignore the recommendations in this section and proceed to the Conditional Access section.]

Security defaults in Microsoft Entra ID make it easier to be secure and help protect your organization. Security defaults contain preconfigured security settings for common attacks.

Security defaults is available to everyone. The goal is to ensure that all organizations have a basic level of security enabled at no extra cost. You may turn on security defaults in the Azure portal.

Rationale:

Security defaults provide secure default settings that we manage on behalf of organizations to keep customers safe until they are ready to manage their own identity security settings.

For example, doing the following:

- Requiring all users and admins to register for MFA.
- Challenging users with MFA - when necessary, based on factors such as location, device, role, and task.
- Disabling authentication from legacy authentication clients, which can’t do MFA.

Impact:

This recommendation should be implemented initially and then may be overridden by other service/product specific CIS Benchmarks. Administrators should also be aware that certain configurations in Microsoft Entra ID may impact other Microsoft services such as Microsoft 365.

Audit:

Audit from Azure Portal
To ensure security defaults is enabled in your directory:

1. From Azure Home select the Portal Menu.
2. Browse to `Microsoft Entra ID` > `Properties`.

3. Select `Manage security defaults`.
4. Under `Security defaults`, verify that `Enabled (recommended)` is selected.

Remediation:

Remediate from Azure Portal
To enable security defaults in your directory:

1. From Azure Home select the Portal Menu.
2. Browse to `Microsoft Entra ID` > `Properties`.
3. Select `Manage security defaults`.
4. Under `Security defaults`, select `Enabled (recommended)`.
5. Select `Save`.

Default Value:

If your tenant was created on or after October 22, 2019, security defaults may already be enabled in your tenant.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults
2. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/introducing-security-defaults/ba-p/1061414
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-2-protect-identity-and-authentication-systems

Additional Information:

This recommendation differs from the Microsoft 365 Benchmark. This is because the potential impact associated with disabling Security Defaults is dependent upon the security settings implemented in the environment. It is recommended that organizations disabling Security Defaults implement appropriate security settings to replace the settings configured by Security Defaults.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

2.1.2 Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users (Manual)

Profile Applicability:

- Level 1

Description:

[**IMPORTANT - Please read the section overview:** If your organization pays for Microsoft Entra ID licensing (included in Microsoft 365 E3, E5, or F5, and EM&S E3 or E5 licenses) and **CAN** use Conditional Access, ignore the recommendations in this section and proceed to the Conditional Access section.]

Enable multi-factor authentication for all roles, groups, and users that have write access or permissions to Azure resources. These include custom created objects or built-in roles such as;

- Service Co-Administrators
- Subscription Owners
- Contributors

Rationale:

Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Impact:

Users would require two forms of authentication before any access is granted. Additional administrative time will be required for managing dual forms of authentication when enabling multi-factor authentication.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select the `Microsoft Entra ID` blade
3. Under `Manage`, click `Roles and administrators`
4. Take note of all users with the role `Service Co-Administrators`, `Owners` or `Contributors`
5. Return to the `Overview`
6. Under `Manage`, click `Users`

7. Click on the `Per-User MFA` button in the top row menu
8. Ensure that `Status` is `Enabled` for all noted users

Audit from REST API
For Every Subscription, For Every Tenant
Step 1: Identify Users with Administrative Access

1. List All Users Using Microsoft Graph API:

```
GET https://graph.microsoft.com/v1.0/users
```

Capture `id` and corresponding `userPrincipalName` ('$uid', '$userPrincipalName')

2. List all Role Definitions Using Azure management API:

```
https://management.azure.com/subscriptions/:subscriptionId/providers/Microsof
t.Authorization/roleDefinitions?api-version=2017-05-01
```

Capture Role Definition IDs/Name ('$name') and role names ('$properties/roleName') where "properties/roleName" contains (`Owner` or `*contributor` or `admin`)

3. List All Role Assignments (Mappings `$A.uid` to `$B.name`) Using Azure Management API:

```
GET
https://management.azure.com/subscriptions/:subscriptionId/providers/Microsof
t.Authorization/roleassignments?api-version=2017-10-01-preview
```

Find all administrative roles (`$B.name`) in `"Properties/roleDefinitionId"` mapped with user ids (`$A.id`) in `"Properties/principalId"` where `"Properties/principalType" == "User"`

4. Now Match (`$CProperties/principalId`) with `$A.uid` and get `$A.userPrincipalName` save this as `D.userPrincipalName`

Step 2: Run Graph PowerShell command:

```
get-mguser -All | where {$_.StrongAuthenticationMethods.Count -eq 0} |
Select-Object -Property UserPrincipalName
```

If the output contains any of the `$D.userPrincipalName`, then this recommendation is non-compliant.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** e3e008c3-56b9-4133-8fd7-d3347377402a **- Name:** 'Accounts with owner permissions on Azure resources should be MFA enabled'
- **Policy ID:** 931e118d-50a1-4457-a5e4-78550e086c52 **- Name:** 'Accounts with write permissions on Azure resources should be MFA enabled'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID` blade
3. Under `Manage`, click `Roles and administrators`
4. Take note of all users with the role `Service Co-Administrators`, `Owners` or `Contributors`
5. Return to the `Overview`
6. Under `Manage`, click `Users`
7. Click on the `Per-User MFA` button in the top row menu
8. Check the box next to each noted user
9. Click `Enable MFA`
10. Click `Enable`

Other Options within Azure Portal

Follow Microsoft Azure documentation and enable multi-factor authentication in your environment.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa
Enabling and configuring MFA with conditional access policy is a multi-step process. Here are some additional resources on the process within Entra ID to enable multi-factor authentication for users within your subscriptions with conditional access policy.
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted#enable-multi-factor-authentication-with-conditional-access
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings

Default Value:

By default, multi-factor authentication is disabled for all users.

References:

1. https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication
2. https://stackoverflow.com/questions/41156206/azure-active-directory-premium-mfa-attributes-via-graph-api
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-4-authenticate-server-and-services

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

2.1.3 Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users (Manual)

Profile Applicability:

- Level 2

Description:

[**IMPORTANT - Please read the section overview:** If your organization pays for Microsoft Entra ID licensing (included in Microsoft 365 E3, E5, or F5, and EM&S E3 or E5 licenses) and **CAN** use Conditional Access, ignore the recommendations in this section and proceed to the Conditional Access section.]

Enable multi-factor authentication for all non-privileged users.

Rationale:

Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

Impact:

Users would require two forms of authentication before any access is granted. Also, this requires an overhead for managing dual forms of authentication.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select the `Microsoft Entra ID` blade
3. Under `Manage`, click `Users`
4. Click the `Per-User MFA` button on the top bar

For every user listed, ensure that the `Status` column indicates `Enabled`

Audit from REST API

For Every Subscription, For Every Tenant

Step 1: Identify Users with non-administrative Access

1. List All Users Using Microsoft Graph API:

```
GET https://graph.microsoft.com/v1.0/users
```

Capture id and corresponding userPrincipalName ($uid, $userPrincipalName)

2. List all Role Definitions Using Azure management API:

```
https://management.azure.com/subscriptions/<subscriptionId>/providers/Microso
ft.Authorization/roleDefinitions?api-version=2017-05-01
```

Capture Role Definition IDs/Name ($name) and role names ($properties/roleName) where "properties/roleName" does NOT contain (Owner or *contributor or admin)

3. List All Role Assignments (Mappings $A.uid to $B.name) Using Azure Management API:

```
GET
https://management.azure.com/subscriptions/<subscriptionId>/providers/Microso
ft.Authorization/roleassignments?api-version=2017-10-01-preview
```

Find all non-administrative roles ($B.name) in "Properties/roleDefinationId" mapped with user ids ($A.id) in "Properties/principalId" where "Properties/principalType" == "User"
D> Now Match ($CProperties/principalId) with $A.uid and get $A.userPrincipalName save this as D.userPrincipleName

Step 2: Run Graph PowerShell command:

```
get-mguser -All | where {$_.StrongAuthenticationMethods.Count -eq 0} |
Select-Object -Property UserPrincipalName
```

If the output contains any of the $D.userPrincipleName, then this recommendation is non-compliant.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 81b3ccb4-e6e8-4e4a-8d05-5df25cd29fd4 **- Name:** 'Accounts with read permissions on Azure resources should be MFA enabled'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Entra ID blade

3. Under `Manage`, click `Users`
4. Click on the `Per-User MFA` button in the top row menu
5. Check the box next to each user
6. Click `Enable MFA`
7. Click `Enable`

Other Options within Azure Portal
Follow Microsoft Azure documentation and enable multi-factor authentication in your environment.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa
Enabling and configuring MFA is a multi-step process. Here are some additional resources on the process within Microsoft Entra ID:
https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-admin-mfa
https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-getstarted#enable-multi-factor-authentication-with-conditional-access
https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-mfasettings

Default Value:

By default, multi-factor authentication is disabled for all users.

References:

1. https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication
2. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-userstates
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-4-authenticate-server-and-services

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

2.1.4 Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled (Manual)

Profile Applicability:

- Level 1

Description:

[**IMPORTANT - Please read the section overview:** If your organization pays for Microsoft Entra ID licensing (included in Microsoft 365 E3, E5, or F5, and EM&S E3 or E5 licenses) and **CAN** use Conditional Access, ignore the recommendations in this section and proceed to the Conditional Access section.]

Do not allow users to remember multi-factor authentication on devices.

Rationale:

Remembering Multi-Factor Authentication (MFA) for devices and browsers allows users to have the option to bypass MFA for a set number of days after performing a successful sign-in using MFA. This can enhance usability by minimizing the number of times a user may need to perform two-step verification on the same device. However, if an account or device is compromised, remembering MFA for trusted devices may affect security. Hence, it is recommended that users not be allowed to bypass MFA.

Impact:

For every login attempt, the user will be required to perform multi-factor authentication.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, click `Users`
4. Click the `Per-user MFA` button on the top bar
5. Click on `Service settings`
6. Ensure that `Allow users to remember multi-factor authentication on devices they trust` is not enabled

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, click `Users`

4. Click the `Per-user MFA` button on the top bar
5. Click on `Service settings`
6. Uncheck the box next to `Allow users to remember multi-factor authentication on devices they trust`
7. Click `Save`

Default Value:

By default, `Allow users to remember multi-factor authentication on devices they trust` is disabled.

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-mfa-mfasettings#remember-multi-factor-authentication-for-devices-that-users-trust
2. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-6-use-strong-authentication-controls

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

2.2 Conditional Access

For most Azure tenants, and certainly for organizations with a significant use of Microsoft Entra ID, Conditional Access policies are recommended and preferred. To use Conditional Access Policies, a licensing plan is required, and **Security Defaults must be disabled**. Because of the licensing requirement, all Conditional Access policies are assigned a profile of "Level 2."

Conditional Access requires one of the following plans:

- Microsoft Entra ID P1 or P2
- Microsoft 365 Business Premium
- Microsoft 365 E3 or E5
- Microsoft 365 F1, F3, F5 Security and F5 Security + Compliance
- Enterprise Mobility & Security E3 or E5

2.2.1 Ensure Trusted Locations Are Defined (Manual)

Profile Applicability:

- Level 2

Description:

Microsoft Entra ID Conditional Access allows an organization to configure `Named locations` and configure whether those locations are trusted or untrusted. These settings provide organizations the means to specify Geographical locations for use in conditional access policies, or define actual IP addresses and IP ranges and whether or not those IP addresses and/or ranges are trusted by the organization.

Rationale:

Defining trusted source IP addresses or ranges helps organizations create and enforce Conditional Access policies around those trusted or untrusted IP addresses and ranges. Users authenticating from trusted IP addresses and/or ranges may have less access restrictions or access requirements when compared to users that try to authenticate to Microsoft Entra ID from untrusted locations or untrusted source IP addresses/ranges.

Impact:

When configuring `Named locations`, the organization can create locations using Geographical location data or by defining source IP addresses or ranges. Configuring `Named locations` using a Country location does not provide the organization the ability to mark those locations as trusted, and any Conditional Access policy relying on those `Countries location` setting will not be able to use the `All trusted locations` setting within the Conditional Access policy. They instead will have to rely on the `Select locations` setting. This may add additional resource requirements when configuring and will require thorough organizational testing.

In general, Conditional Access policies may completely prevent users from authenticating to Microsoft Entra ID, and thorough testing is recommended. To avoid complete lockout, a 'Break Glass' account with full Global Administrator rights is recommended in the event all other administrators are locked out of authenticating to Microsoft Entra ID. This 'Break Glass' account should be excluded from Conditional Access Policies and should be configured with the longest pass phrase feasible in addition to a FIDO2 security key or certificate kept in a very secure physical location. This account should only be used in the event of an emergency and complete administrator lockout.

NOTE: Starting July 2024, Microsoft will begin requiring MFA for All Users - including Break Glass Accounts. By the end of October 2024, this requirement will be enforced. Physical FIDO2 security keys, or a certificate kept on secure removable storage can fulfill this MFA requirement. If opting for a physical device, that device should be kept in a very secure, documented physical location.

Audit:

Audit from Azure Portal

1. In the Azure Portal, navigate to `Microsoft Entra ID`
2. Under `Manage`, click `Security`
3. Under `Protect`, click `Conditional Access`
4. Under `Manage`, click `Named locations`

Ensure there are `IP ranges location` settings configured and marked as `Trusted`

Audit from PowerShell

```
Get-MgIdentityConditionalAccessNamedLocation
```

In the output from the above command, for each Named location group, make sure at least one entry contains the `IsTrusted` parameter with a value of `True`. Otherwise, if there is no output as a result of the above command or all of the entries contain the `IsTrusted` parameter with an empty value, a `NULL` value, or a value of `False`, the results are out of compliance with this check.

Remediation:

Remediate from Azure Portal

1. In the Azure Portal, navigate to `Microsoft Entra ID`
2. Under `Manage`, click `Security`
3. Under `Protect`, click `Conditional Access`
4. Under `Manage`, click `Named locations`
5. Within the `Named locations` blade, click on `IP ranges location`
6. Enter a name for this location setting in the `Name` text box
7. Click on the `+` sign
8. Add an IP Address Range in CIDR notation inside the text box that appears
9. Click on the `Add` button
10. Repeat steps 7 through 9 for each IP Range that needs to be added
11. If the information entered are trusted ranges, select the `Mark as trusted location` check box
12. Once finished, click on `Create`

Remediate from PowerShell

Create a new trusted IP-based Named location policy

```
[System.Collections.Generic.List`1[Microsoft.Open.MSGraph.Model.IpRange]]$ipR
anges = @()
$ipRanges.Add("<first IP range in CIDR notation>")
$ipRanges.Add("<second IP range in CIDR notation>")
$ipRanges.Add("<third IP range in CIDR notation>")
New-MgIdentityConditionalAccessNamedLocation -dataType
"#microsoft.graph.ipNamedLocation" -DisplayName "<name of IP Named location
policy>" -IsTrusted $true -IpRanges $ipRanges
```

Set an existing IP-based Named location policy to trusted

```
Update-MgIdentityConditionalAccessNamedLocation -PolicyId "<ID of the
policy>" -dataType "#microsoft.graph.ipNamedLocation" -IsTrusted $true
```

Default Value:

By default, no locations are configured under the `Named locations` blade within the Microsoft Entra ID Conditional Access blade.

References:

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-assignment-network
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions
3. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	11.1 Maintain Standard Security Configurations for Network Devices Maintain standard, documented security configuration standards for all authorized network devices.		●	●

2.2.2 Ensure that an exclusionary Geographic Access Policy is considered (Manual)

Profile Applicability:

- Level 2

Description:

CAUTION: If these policies are created without first auditing and testing the result, misconfiguration can potentially lock out administrators or create undesired access issues.

Conditional Access Policies can be used to block access from geographic locations that are deemed out-of-scope for your organization or application. The scope and variables for this policy should be carefully examined and defined.

Rationale:

Conditional Access, when used as a deny list for the tenant or subscription, is able to prevent ingress or egress of traffic to countries that are outside of the scope of interest (e.g.: customers, suppliers) or jurisdiction of an organization. This is an effective way to prevent unnecessary and long-lasting exposure to international threats such as APTs.

Impact:

Microsoft Entra ID P1 or P2 is required. Limiting access geographically will deny access to users that are traveling or working remotely in a different part of the world. A point-to-site or site to site tunnel such as a VPN is recommended to address exceptions to geographic access policies.

Audit:

Audit from Azure Portal

1. From Azure Home open the Portal menu in the top left, and select `Microsoft Entra ID`.
2. Scroll down in the menu on the left, and select `Security`.
3. Select on the left side `Conditional Access`.
4. Select `Policies`.
5. Select the policy you wish to audit, then:
   - Under `Assignments` > `Users`, review the users and groups for the personnel the policy will apply to
   - Under `Assignments` > `Target resources`, review the cloud apps or actions for the systems the policy will apply to
   - Under `Conditions` > `Locations`, Review the `Include` locations for those that should be **blocked**

    - Under `Conditions` > `Locations`, Review the `Exclude` locations for those that should be allowed (Note: locations set up in the previous recommendation for Trusted Location should be in the `Exclude` list.)
    - Under `Access Controls` > `Grant` - Confirm that `Block access` is selected.

Audit from Azure CLI

```
As of this writing there are no subcommands for Conditional Access Policies
within the Azure CLI
```

Audit from PowerShell

```
$conditionalAccessPolicies = Get-MgIdentityConditionalAccessPolicy

foreach($policy in $conditionalAccessPolicies) {$policy | Select-Object
@{N='Policy ID'; E={$policy.id}}, @{N="Included Locations";
E={$policy.Conditions.Locations.IncludeLocations}}, @{N="Excluded Locations";
E={$policy.Conditions.Locations.ExcludeLocations}}, @{N="BuiltIn
GrantControls"; E={$policy.GrantControls.BuiltInControls}}}
```

Make sure there is at least 1 row in the output of the above PowerShell command that contains `Block` under the `BuiltIn GrantControls` column and location IDs under the `Included Locations` and `Excluded Locations` columns. If not, a policy containing these options has not been created and is considered a finding.

Remediation:

Remediate from Azure Portal

Part 1 of 2 - Create the policy and enable it in `Report-only` mode.

1. From Azure Home open the portal menu in the top left, and select `Microsoft Entra ID`.
2. Scroll down in the menu on the left, and select `Security`.
3. Select on the left side `Conditional Access`.
4. Select `Policies`.
5. Click the `+ New policy` button, then:
6. Provide a name for the policy.
7. Under `Assignments`, select `Users` then:
    - Under `Include`, select `All users`
    - Under `Exclude`, check Users and groups and only select emergency access accounts and service accounts (**NOTE**: Service accounts are excluded here because service accounts are non-interactive and cannot complete MFA)
8. Under `Assignments`, select `Target resources` then:
    - Under `Include`, select `All cloud apps`
    - Leave `Exclude` blank unless you have a well defined exception
9. Under `Conditions`, select `Locations` then:
    - Select `Include`, then add entries for locations for those that should be **blocked**

    - Select `Exclude`, then add entries for those that should be allowed (**IMPORTANT**: Ensure that all Trusted Locations are in the `Exclude` list.)

10. Under `Access Controls`, select `Grant` select `Block Access`.
11. Set `Enable policy` to `Report-only`.
12. Click `Create`.

Allow some time to pass to ensure the sign-in logs capture relevant conditional access events. These events will need to be reviewed to determine if additional considerations are necessary for your organization (e.g. legitimate locations are being blocked and investigation is needed for exception).
NOTE: The policy is not yet 'live,' since `Report-only` is being used to audit the effect of the policy.
Part 2 of 2 - Confirm that the policy is not blocking access that should be granted, then toggle to `On`.

1. With your policy now in report-only mode, return to the Microsoft Entra blade and click on `Sign-in logs`.
2. Review the recent sign-in events - click an event then review the event details (specifically the `Report-only` tab) to ensure:
    - The sign-in event you're reviewing occurred **after** turning on the policy in report-only mode
    - The policy name from step 6 above is listed in the `Policy Name` column
    - The `Result` column for the new policy shows that the policy was `Not applied` (indicating the location origin was not blocked)
3. If the above conditions are present, navigate back to the policy name in Conditional Access and open it.
4. Toggle the policy from `Report-only` to `On`.
5. Click `Save`.

Remediate from PowerShell

First, set up the conditions objects values before updating an existing conditional access policy or before creating a new one. You may need to use additional PowerShell cmdlets to retrieve specific IDs such as the `Get-MgIdentityConditionalAccessNamedLocation` which outputs the `Location IDs` for use with conditional access policies.

```
$conditions = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessConditionSet

$conditions.Applications = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessApplicationCondition
$conditions.Applications.IncludeApplications = <"All" | "Office365" | "app
ID" | @("app ID 1", "app ID 2", etc...>
$conditions.Applications.ExcludeApplications = <"Office365" | "app ID" |
@("app ID 1", "app ID 2", etc...)>

$conditions.Users = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessUserCondition
$conditions.Users.IncludeUsers = <"All" | "None" | "GuestsOrExternalUsers" |
"Specific User ID" | @("User ID 1", "User ID 2", etc.)>
$conditions.Users.ExcludeUsers = <"GuestsOrExternalUsers" | "Specific User
ID" | @("User ID 1", "User ID 2", etc.)>
$conditions.Users.IncludeGroups = <"group ID" | "All" | @("Group ID 1",
"Group ID 2", etc...)>
$conditions.Users.ExcludeGroups = <"group ID" | @("Group ID 1", "Group ID 2",
etc...)>
$conditions.Users.IncludeRoles = <"Role ID" | "All" | @("Role ID 1", "Role ID
2", etc...)>
$conditions.Users.ExcludeRoles = <"Role ID" | @("Role ID 1", "Role ID 2",
etc...)>

$conditions.Locations = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessLocationCondition
$conditions.Locations.IncludeLocations = <"Location ID" | @("Location ID 1",
"Location ID 2", etc...) >
$conditions.Locations.ExcludeLocations = <"AllTrusted" | "Location ID" |
@("Location ID 1", "Location ID 2", etc...)>


$controls = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessGrantControls
$controls._Operator = "OR"
$controls.BuiltInControls = "block"
```

Next, update the existing conditional access policy with the condition set options configured with the previous commands.

```
Update-MgIdentityConditionalAccessPolicy -PolicyId <policy ID> -Conditions
$conditions -GrantControls $controls
```

To create a new conditional access policy that complies with this best practice, run the following commands after creating the condition set above

```
New-MgIdentityConditionalAccessPolicy -Name "Policy Name" -State
<enabled|disabled> -Conditions $conditions -GrantControls $controls
```

Default Value:

This policy does not exist by default.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location
2. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource in References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	12.1 Maintain an Inventory of Network Boundaries Maintain an up-to-date inventory of all of the organization's network boundaries.	●	●	●

2.2.3 Ensure that an exclusionary Device code flow policy is considered (Manual)

Profile Applicability:

- Level 2

Description:

Conditional Access Policies can be used to prevent the Device code authentication flow. Device code flow should be permitted only for users that regularly perform duties that explicitly require the use of Device Code to authenticate, such as utilizing Azure with PowerShell.

Rationale:

Attackers use Device code flow in phishing attacks and, if successful, results in the attacker gaining access tokens and refresh tokens which are scoped to "user_impersonation", which can perform any action the user has permission to perform.

Impact:

Microsoft Entra ID P1 or P2 is required.

This policy should be tested using the `Report-only mode` before implementation. Without a full and careful understanding of the accounts and personnel who require Device code authentication flow, implementing this policy can block authentication for users and devices who rely on Device code flow. For users and devices that rely on device code flow authentication, more secure alternatives should be implemented wherever possible.

Audit:

Audit from Azure Portal

1. From Azure Home open the Portal menu in the top left and select `Microsoft Entra ID`.
2. Scroll down in the menu on the left and select `Security`.
3. Select on the left side `Conditional Access`.
4. Select `Policies`.
5. Select the policy you wish to audit, then:
    - Under `Assignments` > `Users`, review the users and groups for the personnel the policy will apply to
    - Under `Assignments` > `Target resources`, review the cloud apps or actions for the systems the policy will apply to
    - Under `Conditions` > `Authentication Flows`, review the configuration to ensure `Device code flow` is selected

- Under `Access Controls` > `Grant` - Confirm that `Block access` is selected.

Remediation:

Remediate from Azure Portal
Part 1 of 2 - Create the policy and enable it in `Report-only` mode.

1. From Azure Home open the portal menu in the top left and select `Microsoft Entra ID`.
2. Scroll down in the menu on the left and select `Security`.
3. Select on the left side `Conditional Access`.
4. Select `Policies`.
5. Click the `+ New policy` button, then:
6. Provide a name for the policy.
7. Under `Assignments`, select `Users` then:
   - Under `Include`, select `All users`
   - Under `Exclude`, check Users and groups and only select emergency access accounts
8. Under `Assignments`, select `Target resources` then:
   - Under `Include`, select `All cloud apps`
   - Leave `Exclude` blank unless you have a well defined exception
9. Under `Conditions` > `Authentication Flows`, set Configure to `Yes` then:
   - Select `Device code flow`
   - Select `Done`
10. Under `Access Controls` > `Grant`, select `Block Access`.
11. Set `Enable policy` to `Report-only`.
12. Click `Create`.

Allow some time to pass to ensure the sign-in logs capture relevant conditional access events. These events will need to be reviewed to determine if additional considerations are necessary for your organization (e.g. many legitimate use cases of device code authentication are observed).

NOTE: The policy is not yet 'live,' since `Report-only` is being used to audit the effect of the policy.

Part 2 of 2 - Confirm that the policy is not blocking access that should be granted, then toggle to `On`.

1. With your policy now in report-only mode, return to the Microsoft Entra blade and click on `Sign-in logs`.
2. Review the recent sign-in events - click an event then review the event details (specifically the `Report-only` tab) to ensure:
   - The sign-in event you're reviewing occurred **after** turning on the policy in report-only mode

    - The policy name from step 6 above is listed in the `Policy Name` column
    - The `Result` column for the new policy shows that the policy was `Not applied` (indicating the device code authentication flow was not blocked)
3. If the above conditions are present, navigate back to the policy name in Conditional Access and open it.
4. Toggle the policy from `Report-only` to `On`.
5. Click `Save`.

Default Value:

This policy does not exist by default.

References:

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-authentication-flows#device-code-flow
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions
3. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only
4. https://learn.microsoft.com/en-us/entra/identity/conditional-access/how-to-policy-authentication-flows

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource in References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●
v7	12.4 Deny Communication over Unauthorized Ports Deny communication over unauthorized TCP or UDP ports or application traffic to ensure that only authorized protocols are allowed to cross the network boundary in or out of the network at each of the organization's network boundaries.	●	●	●

2.2.4 Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups (Manual)

Profile Applicability:

- Level 2

Description:

For designated users, they will be prompted to use their multi-factor authentication (MFA) process on login.

Rationale:

Enabling multi-factor authentication is a recommended setting to limit the use of Administrative accounts to authenticated personnel.

Impact:

There is an increased cost, as Conditional Access policies require Microsoft Entra ID P1. Similarly, MFA may require additional overhead to maintain. There is also a potential scenario in which the multi-factor authentication method can be lost, and administrative users are no longer able to log in. For this scenario, there should be an emergency access account. Please see References for creating this.

NOTE: Starting July 2024, Microsoft will begin requiring MFA for All Users - including Break Glass Accounts. By the end of October 2024, this requirement will be enforced. Physical FIDO2 security keys, or a certificate kept on secure removable storage can fulfill this MFA requirement. If opting for a physical device, that device should be kept in a very secure, documented physical location.

Audit:

Audit from Azure Portal

1. From Azure Home open the Portal Menu in the top left, and select `Microsoft Entra ID`.
2. Select `Security`.
3. Select `Conditional Access`.
4. Select `Policies`.
5. Select the policy you wish to audit.
6. Click the blue text under `Users`.
7. View under `Include` the corresponding users and groups to whom the policy is applied. Be certain the emergency access account is not in the list.
8. View under `Exclude` to determine which Users and groups to whom the policy is not applied.

Remediation:

Remediate from Azure Portal

1. From Azure Home open the Portal Menu in top left, and select Microsoft Entra ID.
2. Select `Security`.
3. Select `Conditional Access`.
4. Select `Policies`.
5. Click `+ New policy`.
6. Enter a name for the policy.
7. Click the blue text under `Users`.
8. Select `Select users and groups`.
9. Select administrative groups this policy should apply to and click `Select`.
10. Under `Exclude`, check `Users and groups`.
11. Select users this policy not should apply to and click `Select`.
12. Click the blue text under `Target resources`.
13. Select `All cloud apps`.
14. Click the blue text under `Grant`.
15. Under Grant access, check `Require multifactor authentication` and click `Select`.
16. Set `Enable policy` to `Report-only`.
17. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

Default Value:

Starting October 2024, MFA will be required for all accounts by default.

References:

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-admin-mfa
2. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access
3. https://learn.microsoft.com/en-us/entra/identity/conditional-access/troubleshoot-conditional-access-what-if
4. https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-insights-reporting
5. https://learn.microsoft.com/en-us/entra/identity/conditional-access/plan-conditional-access
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource in References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

2.2.5 Ensure that A Multi-factor Authentication Policy Exists for All Users (Manual)

Profile Applicability:

- Level 2

Description:

For designated users, they will be prompted to use their multi-factor authentication (MFA) process on logins.

Rationale:

Enabling multi-factor authentication is a recommended setting to limit the potential of accounts being compromised and limiting access to authenticated personnel.

Impact:

There is an increased cost, as Conditional Access policies require Microsoft Entra ID P1 or P2. Similarly, this may require additional overhead to maintain if users lose access to their MFA.

NOTE: Starting July 2024, Microsoft will begin requiring MFA for All Users - including Break Glass Accounts. By the end of October 2024, this requirement will be enforced. Physical FIDO2 security keys, or a certificate kept on secure removable storage can fulfill this MFA requirement. If opting for a physical device, that device should be kept in a very secure, documented physical location.

Audit:

Audit from Azure Portal

1. From Azure Home open the Portal Menu in the top left, and select `Microsoft Entra ID`.
2. Scroll down in the menu on the left, and select `Security`.
3. Select on the left side `Conditional Access`.
4. Select `Policies`.
5. Select the policy you wish to audit.
6. Click the blue text under `Users`.
7. View under `Include` the corresponding users and groups to whom the policy is applied.
8. View under `Exclude` to determine which users and groups to whom the policy is not applied.

Remediation:

Remediate from Azure Portal

1. From Azure Home open Portal menu in the top left, and select `Microsoft Entra ID`.
2. Select `Security`.
3. Select `Conditional Access`.
4. Select `Policies`.
5. Click `+ New policy`.
6. Enter a name for the policy.
7. Click the blue text under `Users`.
8. Under `Include`, select `All users`.
9. Under `Exclude`, check `Users and groups`.
10. Select users this policy should not apply to and click `Select`.
11. Click the blue text under `Target resources`.
12. Select `All cloud apps`.
13. Click the blue text under `Grant`.
14. Under `Grant access`, check `Require multifactor authentication` and click `Select`.
15. Set `Enable policy` to `Report-only`.
16. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

Default Value:

Starting October 2024, MFA will be required for all accounts by default.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa
2. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access-what-if
3. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource the in References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

2.2.6 Ensure Multi-factor Authentication is Required for Risky Sign-ins (Manual)

Profile Applicability:

- Level 2

Description:

Entra ID tracks the behavior of sign-in events. If the Entra ID domain is licensed with P2, the sign-in behavior can be used as a detection mechanism for additional scrutiny during the sign-in event. If this policy is set up, then Risky Sign-in events will prompt users to use multi-factor authentication (MFA) tokens on login for additional verification.

Rationale:

Enabling multi-factor authentication is a recommended setting to limit the potential of accounts being compromised and limiting access to authenticated personnel. Enabling this policy allows Entra ID's risk-detection mechanisms to force additional scrutiny on the login event, providing a deterrent response to potentially malicious sign-in events, and adding an additional authentication layer as a reaction to potentially malicious behavior.

Impact:

Risk Policies for Conditional Access require Microsoft Entra ID P2. Additional overhead to support or maintain these policies may also be required if users lose access to their MFA tokens.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu in the top left and select `Microsoft Entra ID`.
2. Select `Security`.
3. Select on the left side `Conditional Access`.
4. Select `Policies`.
5. Select the policy you wish to audit.
6. Click the blue text under `Users`.
7. View under `Include` the corresponding users and groups to whom the policy is applied.
8. View under `Exclude` to determine which users and groups to whom the policy is not applied.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu in the top left and select `Microsoft Entra ID`.
2. Select `Security`
3. Select `Conditional Access`.
4. Select `Policies`.
5. Click `+ New policy`.
6. Enter a name for the policy.
7. Click the blue text under `Users`.
8. Under `Include`, select `All users`.
9. Under `Exclude`, check `Users and groups`.
10. Select users this policy should not apply to and click `Select`.
11. Click the blue text under `Target resources`.
12. Select `All cloud apps`.
13. Click the blue text under `Conditions`.
14. Select `Sign-in risk`.
15. Update the `Configure` toggle to `Yes`.
16. Check the sign-in risk level this policy should apply to, e.g. `High` and `Medium`.
17. Select `Done`.
18. Click the blue text under `Grant` and check `Require multifactor authentication` then click the `Select` button.
19. Click the blue text under `Session` then check `Sign-in frequency` and select `Every time` and click the `Select` button.
20. Set `Enable policy` to `Report-only`.
21. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

Default Value:

MFA is not enabled by default.

References:

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-risk
2. https://learn.microsoft.com/en-us/entra/identity/conditional-access/troubleshoot-conditional-access-what-if
3. https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-insights-reporting
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions

5. https://learn.microsoft.com/en-us/entra/id-protection/overview-identity-protection#license-requirements

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource the in References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

2.2.7 Ensure Multi-factor Authentication is Required for Windows Azure Service Management API (Manual)

Profile Applicability:

- Level 2

Description:

This recommendation ensures that users accessing the Windows Azure Service Management API (i.e. Azure Powershell, Azure CLI, Azure Resource Manager API, etc.) are required to use multi-factor authentication (MFA) credentials when accessing resources through the Windows Azure Service Management API.

Rationale:

Administrative access to the Windows Azure Service Management API should be secured with a higher level of scrutiny to authenticating mechanisms. Enabling multi-factor authentication is recommended to reduce the potential for abuse of Administrative actions, and to prevent intruders or compromised admin credentials from changing administrative settings.

IMPORTANT: While this recommendation allows exceptions to specific Users or Groups, they should be very carefully tracked and reviewed for necessity on a regular interval through an Access Review process. It is important that this rule be built to include "All Users" to ensure that all users not specifically excepted will be required to use MFA to access the Azure Service Management API.

Impact:

Conditional Access policies require Microsoft Entra ID P1 or P2 licenses. Similarly, they may require additional overhead to maintain if users lose access to their MFA. Any users or groups which are granted an exception to this policy should be carefully tracked, be granted only minimal necessary privileges, and conditional access exceptions should be regularly reviewed or investigated.

Audit:

Audit from Azure Portal

1. From the Azure Admin Portal dashboard, open `Microsoft Entra ID`.
2. In the menu on the left of the Entra ID blade, click `Security`.
3. In the menu on the left of the Security blade, click `Conditional Access`.
4. In the menu on the left of the Conditional Access blade, click `Policies`.
5. Click on the name of the policy you wish to audit.
6. Click the blue text under `Users`.
7. Under the `Include` section of Users, ensure that `All Users` is selected.

8. Under the `Exclude` section of Users, review the `Users and Groups` that are excluded from the policy (NOTE: this should be limited to break-glass emergency access accounts, non-interactive service accounts, and other carefully considered exceptions).
9. On the left side, click the blue text under `Target resources`.
10. Under the `Include` section of Target Resources, ensure that the `Select apps` radio button is selected.
11. Under `Select`, ensure that `Windows Azure Service Management API` is listed.

Remediation:

Remediate from Azure Portal

1. From the Azure Admin Portal dashboard, open `Microsoft Entra ID`.
2. Click `Security` in the Entra ID blade.
3. Click `Conditional Access` in the Security blade.
4. Click `Policies` in the Conditional Access blade.
5. Click `+ New policy`.
6. Enter a name for the policy.
7. Click the blue text under `Users`.
8. Under `Include`, select `All users`.
9. Under `Exclude`, check `Users and groups`.
10. Select users or groups to be exempted from this policy (e.g. break-glass emergency accounts, and non-interactive service accounts) then click the `Select` button.
11. Click the blue text under `Target resources`.
12. Under `Include`, click the `Select apps` radio button.
13. Click the blue text under `Select`.
14. Check the box next to `Windows Azure Service Management APIs` then click the `Select` button.
15. Click the blue text under `Grant`.
16. Under `Grant access` check the box for `Require multi-factor authentication` then click the `Select` button.
17. Before creating, set `Enable policy` to `Report-only`.
18. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

Default Value:

MFA is not enabled by default for administrative actions.

References:

1. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions

2. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups
3. https://learn.microsoft.com/en-us/entra/identity/conditional-access/howto-conditional-access-policy-azure-management
4. https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-cloud-apps#windows-azure-service-management-api

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with administrators changing settings until they use an MFA device linked to their accounts. An emergency access account is recommended for this eventuality if all administrators are locked out. Please see the documentation in the references for further information. Similarly further testing can also be done via the insights and reporting resource in References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

2.2.8 Ensure Multi-factor Authentication is Required to access Microsoft Admin Portals (Manual)

Profile Applicability:

- Level 2

Description:

This recommendation ensures that users accessing Microsoft Admin Portals (i.e. Microsoft 365 Admin, Microsoft 365 Defender, Exchange Admin Center, Azure Portal, etc.) are required to use multi-factor authentication (MFA) credentials when logging into an Admin Portal.

Rationale:

Administrative Portals for Microsoft Azure should be secured with a higher level of scrutiny to authenticating mechanisms. Enabling multi-factor authentication is recommended to reduce the potential for abuse of Administrative actions, and to prevent intruders or compromised admin credentials from changing administrative settings.

IMPORTANT: While this recommendation allows exceptions to specific Users or Groups, they should be very carefully tracked and reviewed for necessity on a regular interval through an Access Review process. It is important that this rule be built to include "All Users" to ensure that all users not specifically excepted will be required to use MFA to access Admin Portals.

Impact:

Conditional Access policies require Microsoft Entra ID P1 or P2 licenses. Similarly, they may require additional overhead to maintain if users lose access to their MFA. Any users or groups which are granted an exception to this policy should be carefully tracked, be granted only minimal necessary privileges, and conditional access exceptions should be reviewed or investigated.

Audit:

Audit from Azure Portal

1. From the Azure Admin Portal dashboard, open `Microsoft Entra ID`.
2. In the menu on the left of the Entra ID blade, click `Security`.
3. In the menu on the left of the Security blade, click `Conditional Access`.
4. In the menu on the left of the Conditional Access blade, click `Policies`.
5. Click on the name of the policy you wish to audit.
6. Click the blue text under `Users`.
7. Under the `Include` section of Users, review `Users and Groups` to ensure that `All Users` is selected.

8. Under the `Exclude` section of Users, review the `Users and Groups` that are excluded from the policy (NOTE: this should be limited to break-glass emergency access accounts, non-interactive service accounts, and other carefully considered exceptions).
9. On the left side, click the blue text under `Target Resources`.
10. Under the `Include` section of Target resources, ensure the `Select apps` radio button is selected.
11. Under `Select`, ensure `Microsoft Admin Portals` is listed.

Remediation:

Remediate from Azure Portal

1. From the Azure Admin Portal dashboard, open `Microsoft Entra ID`.
2. Click `Security` in the Entra ID blade.
3. Click `Conditional Access` in the Security blade.
4. Click `Policies` in the Conditional Access blade.
5. Click `+ New policy`.
6. Enter a name for the policy.
7. Click the blue text under `Users`.
8. Under `Include`, select `All users`.
9. Under `Exclude`, check `Users and groups`.
10. Select users or groups to be exempted from this policy (e.g. break-glass emergency accounts, and non-interactive service accounts) then click the `Select` button.
11. Click the blue text under `Target resources`.
12. Under `Include`, click the `Select apps` radio button.
13. Click the blue text under `Select`.
14. Check the box next to `Microsoft Admin Portals` then click the `Select` button.
15. Click the blue text under `Grant`.
16. Under `Grant access` check the box for `Require multifactor authentication` then click the `Select` button.
17. Before creating, set `Enable policy` to `Report-only`.
18. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

Default Value:

MFA is not enabled by default for administrative actions.

References:

1. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-7-restrict-resource-access-based-on--conditions

2. https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups
3. https://learn.microsoft.com/en-us/entra/identity/conditional-access/how-to-policy-mfa-admin-portals

Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with administrators changing settings until they use an MFA device linked to their accounts. An emergency access account is recommended for this eventuality if all administrators are locked out. Please see the documentation in the references for further information. Similarly further testing can also be done via the insights and reporting resource in References which monitors Azure sign ins.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

2.3 Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes' (Automated)

Profile Applicability:

- Level 1

Description:

Require administrators or appropriately delegated users to create new tenants.

Rationale:

It is recommended to only allow an administrator to create new tenants. This prevent users from creating new Microsoft Entra ID or Azure AD B2C tenants and ensures that only authorized users are able to do so.

Impact:

Enforcing this setting will ensure that only authorized users are able to create new tenants.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `User settings`
5. Ensure that `Restrict non-admin users from creating tenants` is set to `Yes`

Audit from PowerShell

```
Import-Module Microsoft.Graph.Identity.SignIns
Connect-MgGraph -Scopes 'Policy.ReadWrite.Authorization'
Get-MgPolicyAuthorizationPolicy | Select-Object -ExpandProperty
DefaultUserRolePermissions | Format-List
```

Review the "DefaultUserRolePermissions" section of the output. Ensure that `AllowedToCreateTenants` is not `"True"`.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `User settings`

5. Set `Restrict non-admin users from creating tenants` to `Yes`
6. Click `Save`

Remediate from PowerShell

```
Import-Module Microsoft.Graph.Identity.SignIns

Connect-MgGraph -Scopes 'Policy.ReadWrite.Authorization'

Select-MgProfile -Name beta

$params = @{
DefaultUserRolePermissions = @{
AllowedToCreateTenants = $false
}
}

Update-MgPolicyAuthorizationPolicy -AuthorizationPolicyId  -BodyParameter
$params
```

References:

1. https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions
2. https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#tenant-creator
3. https://blog.admindroid.com/disable-users-creating-new-azure-ad-tenants-in-microsoft-365/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.4 Ensure Guest Users Are Reviewed on a Regular Basis (Manual)

Profile Applicability:

- Level 1

Description:

Microsoft Entra ID has native and extended identity functionality allowing you to invite people from outside your organization to be guest users in your cloud account and sign in with their own work, school, or social identities.

Rationale:

Guest users are typically added outside your employee on-boarding/off-boarding process and could potentially be overlooked indefinitely. To prevent this, guest users should be reviewed on a regular basis. During this audit, guest users should also be determined to not have administrative privileges.

Impact:

Before removing guest users, determine their use and scope. Like removing any user, there may be unforeseen consequences to systems if an account is removed without careful consideration.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Click on `Add filter`
5. Select `User type`
6. Select `Guest` from the Value dropdown
7. Click `Apply`
8. Audit the listed guest users

Audit from Azure CLI

```
az ad user list --query "[?userType=='Guest']"
```

Ensure all users listed are still required and not inactive.

Audit from Azure PowerShell

```
Get-AzureADUser |Where-Object {$_.UserType -like "Guest"} |Select-Object
DisplayName, UserPrincipalName, UserType -Unique
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** e9ac8f8e-ce22-4355-8f04-99b911d6be52 **- Name:** 'Guest accounts with read permissions on Azure resources should be removed'
- **Policy ID:** 94e1c2ac-cbbe-4cac-a2b5-389c812dee87 **- Name:** 'Guest accounts with write permissions on Azure resources should be removed'
- **Policy ID:** 339353f6-2387-4a45-abe4-7f529d121046 **- Name:** 'Guest accounts with owner permissions on Azure resources should be removed'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Click on `Add filter`
5. Select `User type`
6. Select `Guest` from the Value dropdown
7. Click `Apply`
8. Check the box next to all `Guest` users that are no longer required or are inactive
9. Click `Delete`
10. Click `OK`

Remediate from Azure CLI

Before deleting the user, set it to inactive using the ID from the Audit Procedure to determine if there are any dependent systems.

```
az ad user update --id <exampleaccountid@domain.com> --account-enabled
{false}
```

After determining that there are no dependent systems delete the user.

```
Remove-AzureADUser -ObjectId <exampleaccountid@domain.com>
```

Remediate from Azure PowerShell

Before deleting the user, set it to inactive using the ID from the Audit Procedure to determine if there are any dependent systems.

```
Set-AzureADUser -ObjectId "<exampleaccountid@domain.com>" -AccountEnabled
false
```

After determining that there are no dependent systems delete the user.

```
PS C:\>Remove-AzureADUser -ObjectId exampleaccountid@domain.com
```

Default Value:

By default no guest users are created.

References:

1. https://learn.microsoft.com/en-us/entra/external-id/user-properties
2. https://learn.microsoft.com/en-us/entra/fundamentals/how-to-create-delete-users#delete-a-user
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-4-review-and-reconcile-user-access-regularly
4. https://www.microsoft.com/en-us/security/business/identity-access-management/azure-ad-pricing
5. https://learn.microsoft.com/en-us/entra/identity/monitoring-health/howto-manage-inactive-user-accounts
6. https://learn.microsoft.com/en-us/entra/fundamentals/users-restore

Additional Information:

It is good practice to use a dynamic security group to manage guest users.

To create the dynamic security group:

1. Navigate to the 'Microsoft Entra ID' blade in the Azure Portal
2. Select the 'Groups' item
3. Create new
4. Type of 'dynamic'
5. Use the following dynamic selection rule. "(user.userType -eq "Guest")"
6. Once the group has been created, select access reviews option and create a new access review with a period of monthly and send to relevant administrators for review.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person’s name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	16.6 Maintain an Inventory of Accounts Maintain an inventory of all accounts organized by authentication system.		●	●
v7	16.8 Disable Any Unassociated Accounts Disable any account that cannot be associated with a business process or business owner.	●	●	●

2.5 Ensure That 'Number of methods required to reset' is set to '2' (Manual)

Profile Applicability:

- Level 1

Description:

Ensures that two alternate forms of identification are provided before allowing a password reset.

Rationale:

A Self-service Password Reset (SSPR) through Azure Multi-factor Authentication (MFA) ensures the user's identity is confirmed using two separate methods of identification. With multiple methods set, an attacker would have to compromise both methods before they could maliciously reset a user's password.

Impact:

There may be administrative overhead, as users who lose access to their secondary authentication methods will need an administrator with permissions to remove it. There will also need to be organization-wide security policies and training to teach administrators to verify the identity of the requesting user so that social engineering cannot render this setting useless.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Select `Authentication methods`
6. Ensure that `Number of methods required to reset` is set to `2`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Select `Authentication methods`
6. Set the `Number of methods required to reset` to `2`

7. Click `Save`

Default Value:

By default, the `Number of methods required to reset` is set to "2".

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr
2. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-registration-mfa-sspr-combined
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-6-use-strong-authentication-controls
4. https://learn.microsoft.com/en-us/entra/identity/authentication/passwords-faq#password-reset-registration
5. https://support.microsoft.com/en-us/account-billing/reset-your-work-or-school-password-using-security-info-23dde81f-08bb-4776-ba72-e6b72b9dda9e
6. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

2.6 Ensure that account 'Lockout Threshold' is less than or equal to '10' (Manual)

Profile Applicability:

- Level 1

Description:

The account lockout threshold determines how many failed login attempts are permitted prior to placing the account in a locked-out state and initiating a variable lockout duration.

Rationale:

Account lockout is a method of protecting against brute-force and password spray attacks. Once the lockout threshold has been exceeded, the account enters a locked-out state which prevents all login attempts for a variable duration. The lockout in combination with a reasonable duration reduces the total number of failed login attempts that a malicious actor can execute in a given period of time.

Impact:

If account lockout threshold is set too low (less than 3), users may experience frequent lockout events and the resulting security alerts may contribute to alert fatigue.

If account lockout threshold is set too high (more than 10), malicious actors can programmatically execute more password attempts in a given period of time.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Security`.
4. Under `Manage`, select `Authentication methods`.
5. Under `Manage`, select `Password protection`.
6. Ensure that `Lockout threshold` is set to `10` or fewer.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Security`.
4. Under `Manage`, select `Authentication methods`.

5. Under `Manage`, select `Password protection`.
6. Set the `Lockout threshold` to `10` or fewer.
7. Click `Save`.

Default Value:

By default, Lockout threshold is set to `10`.

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout#manage-microsoft-entra-smart-lockout-values

Additional Information:

NOTE: The variable number for failed login attempts allowed before lockout is prescribed by many security and compliance frameworks. The **appropriate** setting for this variable should be determined by the most restrictive security or compliance framework that your organization follows.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		●	●

2.7 Ensure that account 'Lockout duration in seconds' is greater than or equal to '60' (Manual)

Profile Applicability:

- Level 1

Description:

The account lockout duration value determines how long an account retains the status of lockout, and therefore how long before a user can continue to attempt to login after passing the lockout threshold.

Rationale:

Account lockout is a method of protecting against brute-force and password spray attacks. Once the lockout threshold has been exceeded, the account enters a locked-out state which prevents all login attempts for a variable duration. The lockout in combination with a reasonable duration reduces the total number of failed login attempts that a malicious actor can execute in a given period of time.

Impact:

If account lockout duration is set too low (less than 60 seconds), malicious actors can perform more password spray and brute-force attempts over a given period of time.

If the account lockout duration is set too high (more than 300 seconds) users may experience inconvenient delays during lockout.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Security`.
4. Under `Manage`, select `Authentication methods`.
5. Under `Manage`, select `Password protection`.
6. Ensure that `Lockout duration in seconds` is set to `60` or higher.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Security`.
4. Under `Manage`, select `Authentication methods`.

5. Under `Manage`, select `Password protection`.
6. Set the `Lockout duration in seconds` to `60` or higher.
7. Click `Save`.

Default Value:

By default, Lockout duration in seconds is set to `60`.

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/howto-password-smart-lockout#manage-microsoft-entra-smart-lockout-values

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.10 Enforce Automatic Device Lockout on Portable End-User Devices Enforce automatic device lockout following a predetermined threshold of local failed authentication attempts on portable end-user devices, where supported. For laptops, do not allow more than 20 failed authentication attempts; for tablets and smartphones, no more than 10 failed authentication attempts. Example implementations include Microsoft® InTune Device Lock and Apple® Configuration Profile maxFailedAttempts.		●	●

2.8 Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization (Manual)

Profile Applicability:

- Level 1

Description:

Microsoft Azure provides a Global Banned Password policy that applies to Azure administrative and normal user accounts. This is not applied to user accounts that are synced from an on-premise Active Directory unless Microsoft Entra ID Connect is used and you enable EnforceCloudPasswordPolicyForPasswordSyncedUsers. Please see the list in default values on the specifics of this policy. To further password security, it is recommended to further define a custom banned password policy.

Rationale:

Enabling this gives your organization further customization on what secure passwords are allowed. Setting a bad password list enables your organization to fine-tune its password policy further, depending on your needs. Removing easy-to-guess passwords increases the security of access to your Azure resources.

Impact:

Increasing needed password complexity might increase overhead on administration of user accounts. Licensing requirement for Global Banned Password List and Custom Banned Password list requires Microsoft Entra ID P1 or P2. On-premises Active Directory Domain Services users that are not synchronized to Microsoft Entra ID also benefit from Microsoft Entra ID Password Protection based on existing licensing for synchronized users.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Entra ID`.
3. Under `Manage`, select `Security`.
4. Under `Manage`, select `Authentication methods`.
5. Under `Manage`, select `Password protection`.
6. Ensure `Enforce custom list` is set to `Yes`.
7. Review the list of words banned from use in passwords.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Security`.
4. Under `Manage`, select `Authentication methods`.
5. Under `Manage`, select `Password protection`.
6. Set the `Enforce custom list` option to `Yes`.
7. Click in the `Custom banned password list` text box to add a string.
8. Click `Save`.

Default Value:

By default the custom bad password list is not 'Enabled'. Organizational-specific terms can be added to the custom banned password list, such as the following examples:

- Brand names
- Product names
- Locations, such as company headquarters
- Company-specific internal terms
- Abbreviations that have specific company meaning
- Months and weekdays with your company's local languages

The default Azure bad password policy is already applied to your resources which applies the following basic requirements:

Characters allowed:

- Uppercase characters (A - Z)
- Lowercase characters (a - z)
- Numbers (0 - 9)
- Symbols:
- @ # $ % ^ & * - _ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < >
- blank space

Characters not allowed:

- Unicode characters
- Password length Passwords require
- A minimum of eight characters
- A maximum of 256 characters

Password complexity: Passwords require three out of four of the following categories:

- Uppercase characters
- Lowercase characters
- Numbers
- Symbols Note: Password complexity check isn't required for Education tenants.

Password not recently used:

- When a user changes or resets their password, the new password can't be the same as the current or recently used passwords.
- Password isn't banned by Entra ID Password Protection.
- The password can't be on the global list of banned passwords for Azure AD Password Protection, or on the customizable list of banned passwords specific to your organization.

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad-combined-policy
2. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-password-ban-bad
3. https://docs.microsoft.com/en-us/powershell/module/Azuread/
4. https://www.microsoft.com/en-us/research/publication/password-guidance/
5. https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-configure-custom-password-protection
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-6-use-strong-authentication-controls

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.2 Use Unique Passwords Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	4.4 Use Unique Passwords Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

2.9 Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0' (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that the number of days before users are asked to re-confirm their authentication information is not set to 0.

Rationale:

This setting is necessary if you have setup 'Require users to register when signing in option'. If authentication re-confirmation is disabled, registered users will never be prompted to re-confirm their existing authentication information. If the authentication information for a user changes, such as a phone number or email, then the password reset information for that user reverts to the previously registered authentication information.

Impact:

Users will be prompted for their multifactor authentication at the duration set here.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Under `Manage, select` Registration`
6. Ensure that `Number of days before users are asked to re-confirm their authentication information` is not set to `0`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Under `Manage, select` Registration`
6. Set the `Number of days before users are asked to re-confirm their authentication information` to your organization-defined frequency

7. Click `Save`

Default Value:

By default, the `Number of days before users are asked to re-confirm their authentication information` is set to "180 days".

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#registration
2. https://support.microsoft.com/en-us/account-billing/reset-your-work-or-school-password-using-security-info-23dde81f-08bb-4776-ba72-e6b72b9dda9e
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
4. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-methods

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

2.10 Ensure that 'Notify users on password resets?' is set to 'Yes' (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that users are notified on their primary and alternate emails on password resets.

Rationale:

User notification on password reset is a proactive way of confirming password reset activity. It helps the user to recognize unauthorized password reset activities.

Impact:

Users will receive emails alerting them to password changes to both their primary and alternate emails.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Under `Manage`, select `Notifications`
6. Ensure that `Notify users on password resets?` is set to `Yes`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Under `Manage`, select `Notifications`
6. Set `Notify users on password resets?` to `Yes`
7. Click `Save`

Default Value:

By default, `Notify users on password resets?` is set to "Yes".

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr#set-up-notifications-and-customizations
2. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#notifications
3. https://support.microsoft.com/en-us/account-billing/reset-your-work-or-school-password-using-security-info-23dde81f-08bb-4776-ba72-e6b72b9dda9e
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

2.11 Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes' (Manual)

Profile Applicability:

- Level 1

Description:

Ensure that all Global Administrators are notified if any other administrator resets their password.

Rationale:

Administrator accounts are sensitive. Any password reset activity notification, when sent to all Administrators, ensures that all Global Administrators can passively confirm if such a reset is a common pattern within their group. For example, if all Administrators change their password every 30 days, any password reset activity before that may require administrator(s) to evaluate any unusual activity and confirm its origin.

Impact:

All Global Administrators will receive a notification from Azure every time a password is reset. This is useful for auditing procedures to confirm that there are no out of the ordinary password resets for Administrators. There is additional overhead, however, in the time required for Global Administrators to audit the notifications. This setting is only useful if all Global Administrators pay attention to the notifications and audit each one.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`
5. Under `Manage`, select `Notifications`
6. Ensure that `Notify all admins when other admins reset their password?` is set to `Yes`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `Password reset`

5. Under `Manage`, select `Notifications`
6. Set `Notify all admins when other admins reset their password?` to `Yes`
7. Click `Save`

Default Value:

By default, `Notify all admins when other admins reset their password?` is set to "No".

References:

1. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-sspr-howitworks#notifications
2. https://support.microsoft.com/en-us/account-billing/reset-your-work-or-school-password-using-security-info-23dde81f-08bb-4776-ba72-e6b72b9dda9e
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
5. https://learn.microsoft.com/en-us/entra/identity/authentication/tutorial-enable-sspr#set-up-notifications-and-customizations

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user’s primary, non-privileged account.	●	●	●
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	4.8 Log and Alert on Changes to Administrative Group Membership Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.		●	●

2.12 Ensure `User consent for applications` is set to `Do not allow user consent` (Manual)

Profile Applicability:

- Level 1

Description:

Require administrators to provide consent for applications before use.

Rationale:

If Microsoft Entra ID is running as an identity provider for third-party applications, permissions and consent should be limited to administrators or pre-approved. Malicious applications may attempt to exfiltrate data or abuse privileged user accounts.

Impact:

Enforcing this setting may create additional requests that administrators need to review.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Enterprise applications`
4. Under `Security`, select `Consent and permissions`
5. Under `Manage`, select `User consent settings`
6. Ensure `User consent for applications` is set to `Do not allow user consent`

Audit from PowerShell

```
Connect-MgGraph
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions | Select-Object
-ExpandProperty PermissionGrantPoliciesAssigned
```

If the command returns no values in response, the configuration complies with the recommendation.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Enterprise applications`
4. Under `Security`, select `Consent and permissions`

5. Under `Manage`, select `User consent settings`
6. Set `User consent for applications` to `Do not allow user consent`
7. Click `Save`

Default Value:

By default, `Users consent for applications` is set to `Allow user consent for apps`.

References:

1. https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent?pivots=ms-powershell#configure-user-consent-to-applications
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

2.13 Ensure ‘User consent for applications’ Is Set To ‘Allow for Verified Publishers’ (Manual)

Profile Applicability:

- Level 2

Description:

Allow users to provide consent for selected permissions when a request is coming from a verified publisher.

Rationale:

If Microsoft Entra ID is running as an identity provider for third-party applications, permissions and consent should be limited to administrators or pre-approved. Malicious applications may attempt to exfiltrate data or abuse privileged user accounts.

Impact:

Enforcing this setting may create additional requests that administrators need to review.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Enterprise applications`
4. Under `Security, select` Consent and permissions`
5. Under `Manage`, select `User consent settings`
6. Under `User consent for applications`, ensure `Allow user consent for apps from verified publishers, for selected permissions` is selected

Audit from PowerShell

```
Connect-MgGraph
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions | Select-Object
-ExpandProperty PermissionGrantPoliciesAssigned
```

The command should return either `ManagePermissionGrantsForSelf.microsoft-user-default-low` or a custom app consent policy id if one is in use.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Enterprise applications`

4. Under `Security, select` Consent and permissions`
5. Under `Manage`, select `User consent settings`
6. Under `User consent for applications`, select `Allow user consent for apps from verified publishers, for selected permissions`
7. Click `Save`

Default Value:

By default, `User consent for applications` is set to `Allow user consent for apps`.

References:

1. https://learn.microsoft.com/en-us/entra/identity/enterprise-apps/configure-user-consent?pivots=ms-graph#configure-user-consent-to-applications
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
5. https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/get-mgpolicyauthorizationpolicy?view=graph-powershell-1.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	2.5 Allowlist Authorized Software Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●
v7	2.7 Utilize Application Whitelisting Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.			●

2.14 Ensure That ‘Users Can Register Applications’ Is Set to ‘No’ (Automated)

Profile Applicability:

- Level 1

Description:

Require administrators or appropriately delegated users to register third-party applications.

Rationale:

It is recommended to only allow an administrator to register custom-developed applications. This ensures that the application undergoes a formal security review and approval process prior to exposing Microsoft Entra ID data. Certain users like developers or other high-request users may also be delegated permissions to prevent them from waiting on an administrative user. Your organization should review your policies and decide your needs.

Impact:

Enforcing this setting will create additional requests for approval that will need to be addressed by an administrator. If permissions are delegated, a user may approve a malevolent third party application, potentially giving it access to your data.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `User settings`
5. Ensure that `Users can register applications` is set to `No`

Audit from PowerShell

```
(Get-MgPolicyAuthorizationPolicy).DefaultUserRolePermissions | Format-List
AllowedToCreateApps
```

Command should return the value of `False`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`

3. Under `Manage`, select `Users`
4. Under `Manage`, select `User settings`
5. Set `Users can register applications` to `No`
6. Click `Save`

Remediate from PowerShell

```
$param = @{ AllowedToCreateApps = "$false" }
Update-MgPolicyAuthorizationPolicy -DefaultUserRolePermissions $param
```

Default Value:

By default, `Users can register applications` is set to "Yes".

References:

1. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/delegate-app-roles#restrict-who-can-create-applications
2. https://learn.microsoft.com/en-us/entra/identity-platform/how-applications-are-added#who-has-permission-to-add-applications-to-my-azure-ad-instance
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
5. https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/get-mgpolicyauthorizationpolicy?view=graph-powershell-1.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.3 Address Unauthorized Software Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.	●	●	●
v8	2.4 Utilize Automated Software Inventory Tools Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.		●	●
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	2.6 Address unapproved software Ensure that unauthorized software is either removed or the inventory is updated in a timely manner	●	●	●

2.15 Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' (Automated)

Profile Applicability:

- Level 1

Description:

Limit guest user permissions.

Rationale:

Limiting guest access ensures that guest accounts do not have permission for certain directory tasks, such as enumerating users, groups or other directory resources, and cannot be assigned to administrative roles in your directory. Guest access has three levels of restriction.

1. Guest users have the same access as members (most inclusive),
2. Guest users have limited access to properties and memberships of directory objects (default value),
3. Guest user access is restricted to properties and memberships of their own directory objects (most restrictive).

The recommended option is the 3rd, most restrictive: "Guest user access is restricted to their own directory object".

Impact:

This may create additional requests for permissions to access resources that administrators will need to approve.

According to https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/users-restrict-guest-permissions#services-currently-not-supported

Service without current support might have compatibility issues with the new guest restriction setting.

- Forms
- Project
- Yammer
- Planner in SharePoint

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `External Identities`
4. Select `External collaboration settings`
5. Under `Guest user access`, ensure that `Guest user access restrictions` is set to `Guest user access is restricted to properties and memberships of their own directory objects`

Audit from PowerShell

1. Enter the following:

```
Connect-MgGraph
(Get-MgPolicyAuthorizationPolicy).GuestUserRoleId
```

Which will give a result like:

```
Id                                                : authorizationPolicy
OdataType                                         :
Description                                       : Used to manage
authorization related settings across the company.
DisplayName                                       : Authorization Policy
EnabledPreviewFeatures                            : {}
GuestUserRoleId                                   : 10dae51f-b6af-4016-8d66-
8c2a99b929b3
PermissionGrantPolicyIdsAssignedToDefaultUserRole : {user-default-legacy}
```

If the GuestUserRoleID property does not equal `2af84b1e-32c8-42b7-82bc-daa82404023b` then it is not set to most restrictive.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `External Identities`
4. Select `External collaboration settings`
5. Under `Guest user access`, set `Guest user access restrictions` to `Guest user access is restricted to properties and memberships of their own directory objects`
6. Click `Save`

Remediate from PowerShell

1. Enter the following to update the policy ID:

```
Update-MgPolicyAuthorizationPolicy -GuestUserRoleId "2af84b1e-32c8-42b7-82bc-
daa82404023b"
```

2. Check the GuestUserRoleId again:

```
(Get-MgPolicyAuthorizationPolicy).GuestUserRoleId
```

3. Ensure that the GuestUserRoleId is equal to the earlier entered value of `2af84b1e-32c8-42b7-82bc-daa82404023b`.

Default Value:

By default, `Guest user access restrictions` is set to `Guest users have limited access to properties and memberships of directory objects`.

References:

1. https://learn.microsoft.com/en-us/entra/fundamentals/users-default-permissions#member-and-guest-users
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
5. https://learn.microsoft.com/en-us/entra/identity/users/users-restrict-guest-permissions

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.16 Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users' (Automated)

Profile Applicability:

- Level 2

Description:

Restrict invitations to users with specific administrative roles only.

Rationale:

Restricting invitations to users with specific administrator roles ensures that only authorized accounts have access to cloud resources. This helps to maintain "Need to Know" permissions and prevents inadvertent access to data.

By default the setting `Guest invite restrictions` is set to `Anyone in the organization can invite guest users including guests and non-admins`. This would allow anyone within the organization to invite guests and non-admins to the tenant, posing a security risk.

Impact:

With the option of `Only users assigned to specific admin roles can invite guest users` selected, users with specific admin roles will be in charge of sending invitations to the external users, requiring additional overhead by them to manage user accounts. This will mean coordinating with other departments as they are onboarding new users.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `External Identities`
4. Select `External collaboration settings`
5. Under `Guest invite settings`, for `Guest invite restrictions`, ensure that `Only users assigned to specific admin roles can invite guest users` is selected

Note: This setting has 4 levels of restriction, which include:

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive),

- Member users and users assigned to specific admin roles can invite guest users including guests with member permissions,
- Only users assigned to specific admin roles can invite guest users,
- No one in the organization can invite guest users including admins (most restrictive).

Audit from PowerShell

Enter the following:

```
Connect-MgGraph
(Get-MgPolicyAuthorizationPolicy).AllowInvitesFrom
```

If the resulting value is `adminsAndGuestInviters` the configuration complies.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `External Identities`
4. Select `External collaboration settings`
5. Under `Guest invite settings`, set `Guest invite restrictions`, to `Only users assigned to specific admin roles can invite guest users`
6. Click `Save`

Remediate from PowerShell

Enter the following:

```
Connect-MgGraph
Update-MgPolicyAuthorizationPolicy -AllowInvitesFrom "adminsAndGuestInviters"
```

Default Value:

By default, `Guest invite restrictions` is set to `Anyone in the organization can invite guest users including guests and non-admins`

References:

1. https://learn.microsoft.com/en-us/entra/external-id/external-collaboration-settings-configure
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements

5. https://learn.microsoft.com/en-us/powershell/module/microsoft.graph.identity.signins/update-mgpolicyauthorizationpolicy?view=graph-powershell-1.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

2.17 Ensure That 'Restrict access to Microsoft Entra admin center' is Set to 'Yes' (Manual)

Profile Applicability:

- Level 1

Description:

Restrict access to the Microsoft Entra ID administration center to administrators only.

NOTE: This only affects access to the Entra ID administrator's web portal. This setting does not prohibit privileged users from using other methods such as Rest API or Powershell to obtain sensitive information from Microsoft Entra ID.

Rationale:

The Microsoft Entra ID administrative center has sensitive data and permission settings. All non-administrators should be prohibited from accessing any Microsoft Entra ID data in the administration center to avoid exposure.

Impact:

All administrative tasks will need to be done by Administrators, causing additional overhead in management of users and resources.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `User settings`
5. Under `Administration centre`, ensure that `Restrict access to Microsoft Entra admin center` is set to `Yes`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Users`
4. Under `Manage`, select `User settings`
5. Under `Administration centre`, set `Restrict access to Microsoft Entra admin center` to `Yes`
6. Click `Save`

Default Value:

By default, `Restrict access to Microsoft Entra admin center` is set to `No`

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-assign-admin-roles-azure-portal
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.18 Ensure that 'Restrict user ability to access groups features in the Access Pane' is Set to 'Yes' (Manual)

Profile Applicability:

- Level 2

Description:

Restrict access to group web interface in the Access Panel portal.

Rationale:

Self-service group management enables users to create and manage security groups or Office 365 groups in Microsoft Entra ID. Unless a business requires this day-to-day delegation for some users, self-service group management should be disabled. Any user can access the Access Panel, where they can reset their passwords, view their information, etc. By default, users are also allowed to access the Group feature, which shows groups, members, related resources (SharePoint URL, Group email address, Yammer URL, and Teams URL). By setting this feature to 'Yes', users will no longer have access to the web interface, but still have access to the data using the API. This is useful to prevent non-technical users from enumerating groups-related information, but technical users will still be able to access this information using APIs.

Impact:

Setting to `Yes` could create administrative overhead by customers seeking certain group memberships that will have to be manually managed by administrators with appropriate permissions.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Self Service Group Management`, ensure that `Restrict user ability to access groups features in My Groups` is set to `Yes`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`

4. Under Settings, select General
5. Under Self Service Group Management, set Restrict user ability to access groups features in My Groups to Yes
6. Click Save

Default Value:

By default, Restrict user ability to access groups features in the Access Pane is set to No

References:

1. https://learn.microsoft.com/en-us/entra/identity/users/groups-self-service-management
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.19 Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No' (Manual)

Profile Applicability:

- Level 2

Description:

Restrict security group creation to administrators only.

Rationale:

When creating security groups is enabled, all users in the directory are allowed to create new security groups and add members to those groups. Unless a business requires this day-to-day delegation, security group creation should be restricted to administrators only.

Impact:

Enabling this setting could create a number of requests that would need to be managed by an administrator.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Security Groups`, ensure that `Users can create security groups in Azure portals, API or PowerShell` is set to `No`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Security Groups`, set `Users can create security groups in Azure portals, API or PowerShell` to `No`
6. Click `Save`

Default Value:

By default, `Users can create security groups in Azure portals, API or PowerShell` is set to `Yes`

References:

1. https://learn.microsoft.com/en-us/entra/identity/users/groups-self-service-management#making-a-group-available-for-end-user-self-service
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.20 Ensure that 'Owners can manage group membership requests in My Groups' is set to 'No' (Manual)

Profile Applicability:

- Level 2

Description:

Restrict security group management to administrators only.

Rationale:

Restricting security group management to administrators only prohibits users from making changes to security groups. This ensures that security groups are appropriately managed and their management is not delegated to non-administrators.

Impact:

Group Membership for user accounts will need to be handled by Admins and cause administrative overhead.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Self Service Group Management`, ensure that `Owners can manage group membership requests in My Groups` is set to `No`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Self Service Group Management`, set `Owners can manage group membership requests in My Groups` to `No`
6. Click `Save`

Default Value:

By default, `Owners can manage group membership requests in My Groups` is set to `No`.

References:

1. https://learn.microsoft.com/en-us/entra/identity/users/groups-self-service-management#making-a-group-available-for-end-user-self-service
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-8-determine-access-process-for-cloud-provider-support
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.21 Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No' (Manual)

Profile Applicability:

- Level 2

Description:

Restrict Microsoft 365 group creation to administrators only.

Rationale:

Restricting Microsoft 365 group creation to administrators only ensures that creation of Microsoft 365 groups is controlled by the administrator. Appropriate groups should be created and managed by the administrator and group creation rights should not be delegated to any other user.

Impact:

Enabling this setting could create a number of requests that would need to be managed by an administrator.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Microsoft 365 Groups`, ensure that `Users can create Microsoft 365 groups in Azure portals, API or PowerShell` is set to `No`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Groups`
4. Under `Settings`, select `General`
5. Under `Microsoft 365 Groups`, set `Users can create Microsoft 365 groups in Azure portals, API or PowerShell` to `No`
6. Click `Save`

Default Value:

By default, `Users can create Microsoft 365 groups in Azure portals, API or PowerShell` is set to `Yes`.

References:

1. https://learn.microsoft.com/en-us/microsoft-365/solutions/manage-creation-of-groups?view=o365-worldwide&redirectSourcePath=%252fen-us%252farticle%252fControl-who-can-create-Office-365-Groups-4c46c8cb-17d0-44b5-9776-005fced8e618
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.22 Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes' (Manual)

Profile Applicability:

- Level 1

Description:

NOTE: This recommendation is only relevant if your subscription is using Per-User MFA. If your organization is licensed to use Conditional Access, the preferred method of requiring MFA to join devices to Entra ID is to use a Conditional Access policy (see additional information below for link).

Joining or registering devices to Microsoft Entra ID should require multi-factor authentication.

Rationale:

Multi-factor authentication is recommended when adding devices to Microsoft Entra ID. When set to `Yes`, users who are adding devices from the internet must first use the second method of authentication before their device is successfully added to the directory. This ensures that rogue devices are not added to the domain using a compromised user account.

Impact:

A slight impact of additional overhead, as Administrators will now have to approve every access to the domain.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Devices`
4. Under `Manage`, select `Device settings`
5. Under `Microsoft Entra join and registration settings`, ensure that `Require Multifactor Authentication to register or join devices with Microsoft Entra` is set to `Yes`

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`

3. Under `Manage`, select `Devices`
4. Under `Manage`, select `Device settings`
5. Under `Microsoft Entra join and registration settings`, set `Require Multifactor Authentication to register or join devices with Microsoft Entra` to `Yes`
6. Click `Save`

Default Value:

By default, `Require Multifactor Authentication to register or join devices with Microsoft Entra` is set to `No`.

References:

1. https://learn.microsoft.com/en-us/entra/identity/conditional-access/how-to-policy-mfa-device-register-join
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-6-use-strong-authentication-controls

Additional Information:

If Conditional Access is available, this recommendation should be bypassed in favor of the Conditional Access implementation of requiring Multifactor Authentication to register or join devices with Microsoft Entra.

https://learn.microsoft.com/en-us/entra/identity/conditional-access/how-to-policy-mfa-device-register-join

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.3 Require MFA for Externally-Exposed Applications Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	6.4 Require MFA for Remote Network Access Require MFA for remote network access.	●	●	●
v7	16.3 Require Multi-factor Authentication Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

2.23 Ensure That No Custom Subscription Administrator Roles Exist (Automated)

Profile Applicability:

- Level 1

Description:

The principle of least privilege should be followed and only necessary privileges should be assigned instead of allowing full administrative access.

Rationale:

Custom roles in Azure with administrative access can obfuscate the permissions granted and introduce complexity and blind spots to the management of privileged identities. For less mature security programs without regular identity audits, the creation of Custom roles should be avoided entirely. For more mature security programs with regular identity audits, Custom Roles should be audited for use and assignment, used minimally, and the principle of least privilege should be observed when granting permissions

Impact:

Subscriptions will need to be handled by Administrators with permissions.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Subscriptions`.
3. Select a subscription.
4. Select `Access control (IAM)`.
5. Select `Roles`.
6. Click `Type` and select `Custom role` from the drop-down menu.
7. Select `View` next to a role.
8. Select `JSON`.
9. Check for `assignableScopes` set to the subscription, and `actions` set to `*`.
10. Repeat steps 7-9 for each custom role.

Audit from Azure CLI

List custom roles:

```
az role definition list --custom-role-only True
```

Check for entries with `assignableScope` of the `subscription`, and an action of `*`

Audit from PowerShell

```
Connect-AzAccount
Get-AzRoleDefinition |Where-Object {($_.IsCustom -eq $true) -and
($_.Actions.contains('*'))}
```

Check the output for `AssignableScopes` value set to the subscription.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** a451c1ef-c6ca-483d-87ed-f49761e3ffb5 **- Name:** 'Audit usage of custom RBAC roles'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Subscriptions`.
3. Select a subscription.
4. Select `Access control (IAM)`.
5. Select `Roles`.
6. Click `Type` and select `Custom role` from the drop-down menu.
7. Check the box next to each role which grants subscription administrator privileges.
8. Select `Delete`.
9. Select `Yes`.

Remediate from Azure CLI

List custom roles:

```
az role definition list --custom-role-only True
```

Check for entries with `assignableScope` of the `subscription`, and an action of `*`.
To remove a violating role:

```
az role definition delete --name <role name>
```

Note that any role assignments must be removed before a custom role can be deleted. Ensure impact is assessed before deleting a custom role granting subscription administrator privileges.

Default Value:

By default, no custom owner roles are created.

References:

1. https://docs.microsoft.com/en-us/azure/billing/billing-add-change-azure-subscription-administrator
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-7-follow-just-enough-administration-least-privilege-principle

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user’s primary, non-privileged account.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

2.24 Ensure a Custom Role is Assigned Permissions for Administering Resource Locks (Manual)

Profile Applicability:

- Level 2

Description:

Resource locking is a powerful protection mechanism that can prevent inadvertent modification/deletion of resources within Azure subscriptions/Resource Groups and is a recommended NIST configuration.

Rationale:

Given the resource lock functionality is outside of standard Role Based Access Control(RBAC), it would be prudent to create a resource lock administrator role to prevent inadvertent unlocking of resources.

Impact:

By adding this role, specific permissions may be granted for managing just resource locks rather than needing to provide the wide Owner or User Access Administrator role, reducing the risk of the user being able to do unintentional damage.

Audit:

Audit from Azure Portal

1. In the Azure portal, open a subscription or resource group where you want to view assigned roles.
2. Select `Access control (IAM)`
3. Select `Roles`
4. Search for the custom role named <role_name> e.g. from remediation `Resource Lock Administrator`
5. Ensure that the role is assigned to the appropriate users.

Remediation:

Remediate from Azure Portal

1. In the Azure portal, open a subscription or resource group where you want the custom role to be assigned.
2. Select `Access control (IAM)`.
3. Click `Add`.
4. Select `Add custom role`.
5. In the `Custom role name` field enter `Resource Lock Administrator`.
6. In the Description field enter `Can Administer Resource Locks`.

7. For Baseline permissions select Start from scratch
8. Select Next.
9. In the Permissions tab select Add permissions.
10. In the Search for a permission box, type in Microsoft.Authorization/locks to search for permissions.
11. Click on the result.
12. Check the box next to Permission.
13. Select Add.
14. Select Review + create.
15. Select Create.
16. Assign the newly created role to the appropriate user.

Remediate from PowerShell:
Below is a power shell definition for a resource lock administrator role created at an Azure Management group level

```
Import-Module Az.Accounts
Connect-AzAccount

$role = Get-AzRoleDefinition "User Access Administrator"
$role.Id = $null
$role.Name = "Resource Lock Administrator"
$role.Description = "Can Administer Resource Locks"
$role.Actions.Clear()
$role.Actions.Add("Microsoft.Authorization/locks/*")
$role.AssignableScopes.Clear()

* Scope at the Management group level Management group

$role.AssignableScopes.Add("/providers/Microsoft.Management/managementGroups/
MG-Name")

New-AzRoleDefinition -Role $role
Get-AzureRmRoleDefinition "Resource Lock Administrator"
```

References:

1. https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles
2. https://docs.microsoft.com/en-us/azure/role-based-access-control/check-access
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-7-follow-just-enough-administration-least-privilege-principle
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
7. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

2.25 Ensure That 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' Is Set To 'Permit no one' (Manual)

Profile Applicability:

- Level 2

Description:

Users who are set as subscription owners are able to make administrative changes to the subscriptions and move them into and out of Microsoft Entra ID.

Rationale:

Permissions to move subscriptions in and out of a Microsoft Entra tenant must only be given to appropriate administrative personnel. A subscription that is moved into a Microsoft Entra tenant may be within a folder to which other users have elevated permissions. This prevents loss of data or unapproved changes of the objects within by potential bad actors.

Impact:

Subscriptions will need to have these settings turned off to be moved.

Audit:

Audit from Azure Portal

1. From the Azure Portal Home select the portal menu
2. Select `Subscriptions`
3. In the `Advanced options` drop-down menu, select `Manage Policies`
4. Ensure `Subscription leaving Microsoft Entra tenant` and `Subscription entering Microsoft Entra tenant` are set to `Permit no one`

Remediation:

Remediate from Azure Portal

1. From the Azure Portal Home select the portal menu
2. Select `Subscriptions`
3. In the `Advanced options` drop-down menu, select `Manage Policies`
4. Set `Subscription leaving Microsoft Entra tenant` and `Subscription entering Microsoft Entra tenant` to `Permit no one`
5. Click `Save changes`

Default Value:

By default `Subscription leaving Microsoft Entra tenant` and `Subscription entering Microsoft Entra tenant` are set to `Allow everyone (default)`

References:

1. https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/manage-azure-subscription-policy
2. https://learn.microsoft.com/en-us/entra/fundamentals/how-subscriptions-associated-directory
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-2-protect-identity-and-authentication-systems

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	6.1 Establish an Access Granting Process Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	4.3 Ensure the Use of Dedicated Administrative Accounts Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.	●	●	●

2.26 Ensure fewer than 5 users have global administrator assignment (Manual)

Profile Applicability:

- Level 1

Description:

This recommendation aims to maintain a balance between security and operational efficiency by ensuring that a minimum of 2 and a maximum of 4 users are assigned the Global Administrator role in Microsoft Entra ID. Having at least two Global Administrators ensures redundancy, while limiting the number to four reduces the risk of excessive privileged access.

Rationale:

The Global Administrator role has extensive privileges across all services in Microsoft Entra ID. The Global Administrator role should never be used in regular daily activities; administrators should have a regular user account for daily activities, and a separate account for administrative responsibilities. Limiting the number of Global Administrators helps mitigate the risk of unauthorized access, reduces the potential impact of human error, and aligns with the principle of least privilege to reduce the attack surface of an Azure tenant. Conversely, having at least two Global Administrators ensures that administrative functions can be performed without interruption in case of unavailability of a single admin.

Impact:

Implementing this recommendation may require changes in administrative workflows or the redistribution of roles and responsibilities. Adequate training and awareness should be provided to all Global Administrators.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Roles and administrators`
4. Under `Administrative Roles`, select `Global Administrator`
5. Ensure less than 5 users are actively assigned the role.
6. Ensure that at least 2 users are actively assigned the role.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Entra ID`
3. Under `Manage`, select `Roles and administrators`
4. Under `Administrative Roles`, select `Global Administrator`

If more than 4 users are assigned:

1. Remove Global Administrator role for users which do not or no longer require the role.
2. Assign Global Administrator role via PIM which can be activated when required.
3. Assign more granular roles to users to conduct their duties.

If only one user is assigned:

1. Provide the Global Administrator role to a trusted user or create a break glass admin account.

References:

1. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/best-practices#5-limit-the-number-of-global-administrators-to-less-than-5
2. https://learn.microsoft.com/en-us/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide#security-guidelines-for-assigning-roles
3. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/security-emergency-access
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.1 Establish and Maintain an Inventory of Accounts Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v7	4.1 Maintain Inventory of Administrative Accounts Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.		●	●

3 Security

This section covers security best practice recommendations for products in the Azure Security services category.

Azure Product Category Page: https://azure.microsoft.com/en-us/products/category/security

3.1 Microsoft Defender for Cloud

This subsection provides guidance on the use of Microsoft Defender for Cloud and associated product plans. This guidance is intended to ensure that - at a minimum - the protective measures offered by these plans are being considered. Organizations may find that they have existing products or services that provide the same utility as some Microsoft Defender for Cloud products. Security and Administrative personnel need to make the determination on their organization's behalf regarding which - if any - of these recommendations are relevant to their organization's needs. In consideration of the above, and because of the potential for increased cost and complexity, please be aware that all Microsoft Defender for Cloud and associated plan recommendations are profiled as "Level 2" recommendations.

3.1.1 Microsoft Cloud Security Posture Management (CSPM)

Microsoft Defender for Cloud offers foundational and advanced Cloud Security Posture Management (CSPM) solutions to protect across multi-cloud and hybrid environments. Both solutions cover PaaS as well as IaaS. CSPM provides reporting functionality on security and regulatory frameworks including NIST 800 series, ISO 27001, PCI-DSS, CIS Benchmarks and Controls, and many more. CSPM also provides the ability to create your own custom framework, but this will require significant work. Regulatory standards are reported in a compliance dashboard which offers a summarized view against deployed standards and presents the ability to download compliance reports in various formats.

CSPM has two types of implementations:

1. Foundational (Free): This implementation is free and enabled by default with a limited set of features including:

- Continuous assessment of the security configuration of cloud resources
- Security recommendations to fix misconfigurations and weaknesses
- Secure score summarizing current overall security posture

2. Full CSPM (Paid): Full CSPM is a paid product offering additional functionality including:

- Identity and role assignments discovery
- Network exposure detection
- Attack path analysis
- Cloud security explorer for risk hunting
- Agentless vulnerability scanning
- Agentless secrets scanning
- Governance rules to drive timely remediation and accountability
- Regulatory compliance and industry best practices
- Data-aware security posture
- Agentless discovery for Kubernetes
- Agentless container vulnerability assessment

It is recommended that for full CSPM a cost review is undertaken particularly if your tenant is heavy on IaaS prior to implementing and matched to security requirements.

3.1.1.1 Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On' (Automated)

Profile Applicability:

- Level 1

Description:

Enable automatic provisioning of the monitoring agent to collect security data.

DEPRECATION PLANNED: The Log Analytics Agent is slated for deprecation in August 2024. The Microsoft Defender for Endpoint agent, in tandem with new agentless capabilities will be providing replacement functionality. More detail is available here: https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/microsoft-defender-for-cloud-strategy-and-plan-towards-log/ba-p/3883341.

Rationale:

When `Log Analytics agent for Azure VMs` is turned on, Microsoft Defender for Cloud provisions the Microsoft Monitoring Agent on all existing supported Azure virtual machines and any new ones that are created. The Microsoft Monitoring Agent scans for various security-related configurations and events such as system updates, OS vulnerabilities, endpoint protection, and provides alerts.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Select a subscription
5. Click on `Settings & monitoring`
6. Ensure that `Log Analytics agent` is set to `On`

Repeat the above for any additional subscriptions.

Audit from Azure CLI

Ensure the output of the below command is `On`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<subscriptionID>/providers/Microso
ft.Security/autoProvisioningSettings?api-version=2017-08-01-preview' | jq
'.|.value[] | select(.name=="default")'|jq '.properties.autoProvision'
```

Audit from PowerShell

```
Connect-AzAccount
Get-AzSecurityAutoProvisioningSetting | Select-Object Name, AutoProvision
```

Ensure output for `Id Name AutoProvision` is `/subscriptions//providers/Microsoft.Security/autoProvisioningSettings/default default On`

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 475aae12-b88a-4572-8b36-9b712b2b3a17 **- Name:** 'Auto provisioning of the Log Analytics agent should be enabled on your subscription'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Select a subscription
5. Click on `Settings & monitoring`
6. Set the `Status` of `Log Analytics agent` to `On`
7. Select a Workspace
8. Click `Apply`
9. Click `Continue`

Repeat the above for any additional subscriptions.

Remediate from Azure CLI

Use the below command to set `Automatic provisioning of monitoring agent` to `On`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/subscriptionID/providers/Microsoft
.Security/autoProvisioningSettings/default?api-version=2017-08-01-preview -
d@"input.json"'
```

Where `input.json` contains the Request body json data as mentioned below.

```
   {
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/autoProvi
sioningSettings/default",
  "name": "default",
  "type": "Microsoft.Security/autoProvisioningSettings",
  "properties": {
    "autoProvision": "On"
  }
}
```

Default Value:

By default, `Automatic provisioning of monitoring agent` is set to `On`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-data-security
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/list
6. https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/create
7. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-5-centralize-security-log-management-and-analysis
8. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
9. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification

Additional Information:

- Excluding any of the entries in `input.json` may disable the specific setting by default
- Microsoft has recently changed APIs to get and Update Automatic Provisioning Setting. This recommendation is updated accordingly.

DEPRECATION PLANNED: The Log Analytics Agent is slated for deprecation in August 2024. The Microsoft Defender for Endpoint agent, in tandem with new agentless capabilities will be providing replacement functionality. More detail is available here: https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/microsoft-defender-for-cloud-strategy-and-plan-towards-log/ba-p/3883341.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.1.2 Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected (Automated)

Profile Applicability:

- Level 2

Description:

This integration setting enables Microsoft Defender for Cloud Apps (formerly 'Microsoft Cloud App Security' or 'MCAS' - see additional info) to communicate with Microsoft Defender for Cloud.

Rationale:

Microsoft Defender for Cloud offers an additional layer of protection by using Azure Resource Manager events, which is considered to be the control plane for Azure. By analyzing the Azure Resource Manager records, Microsoft Defender for Cloud detects unusual or potentially harmful operations in the Azure subscription environment. Several of the preceding analytics are powered by Microsoft Defender for Cloud Apps. To benefit from these analytics, subscription must have a Cloud App Security license.

Microsoft Defender for Cloud Apps works only with Standard Tier subscriptions.

Impact:

Microsoft Defender for Cloud Apps works with Standard pricing tier Subscription. Choosing the Standard pricing tier of Microsoft Defender for Cloud incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment Settings`.
4. Click on the subscription name.
5. Select the `Integrations` blade.
6. Ensure setting `Allow Microsoft Defender for Cloud Apps to access my data` is selected.

Audit from Azure CLI

Ensure the output of the below command is `true`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<subscription_ID>/providers/Micros
oft.Security/settings?api-version=2021-06-01' | jq '.|.value[] |
select(.name=="MCAS")'|jq '.properties.enabled'
```

Audit from PowerShell

Run the following series of commands to audit this configuration

```
Get-AzAccount
Set-AzContext -Subscription <subscription ID>
Get-AzSecuritySetting | Select-Object name,enabled |where-object {$_.name -eq
"MCAS"}
```

PowerShell Output - Non-Compliant

```
Name Enabled
---- -------
MCAS    False
```

PowerShell Output - Compliant

```
Name Enabled
---- -------
MCAS    True
```

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment Settings`.
4. Select the subscription.
5. Select `Integrations`.
6. Check `Allow Microsoft Defender for Cloud Apps to access my data`.
7. Select `Save`.

Remediate from Azure CLI

Use the below command to enable Standard pricing tier for Storage Accounts

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<subscription_ID>/providers/Micros
oft.Security/settings/MCAS?api-version=2021-06-01 -d@"input.json"'
```

Where input.json contains the Request body json data as mentioned below.

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/settings/
MCAS",
  "kind": "DataExportSetting",
  "type": "Microsoft.Security/settings",
  "properties": {
    "enabled": true
  }
}
```

Default Value:

With Cloud App Security license, these alerts are enabled by default.

References:

1. https://docs.microsoft.com/en-in/azure/security-center/security-center-alerts-service-layer#azure-management-layer-azure-resource-manager-preview
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/settings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/settings/update
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-9-secure-user-access-to--existing-applications

Additional Information:

NOTE: "Microsoft Defender for Cloud Apps" ("MDCA") is formerly known as "Microsoft Cloud App Security" ("MCAS"). There are a number of places (e.g. Azure CLI) where the "MCAS" acronym is still used within Azure.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v8	13.10 Perform Application Layer Filtering Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			●

Controls Version	Control	IG 1	IG 2	IG 3
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.2 Defender Plan: APIs

Defender for APIs in Microsoft Defender for Cloud offers full lifecycle protection, detection, and response coverage for APIs. Defender for APIs helps you to gain visibility into business-critical APIs. You can investigate and improve your API security posture, prioritize vulnerability fixes, and quickly detect active real-time threats. Defender for API's requires additional configuration in the Microsoft API portal.

Note: There is a cost attached to using Defender for APi

3.1.3 Defender Plan: Servers

3.1.3.1 Ensure That Microsoft Defender for Servers Is Set to 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for Servers enables threat detection for Servers, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for Servers allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Impact:

Turning on Microsoft Defender for Servers in Microsoft Defender for Cloud incurs an additional cost per resource.

Two Defender for Servers plans exist:

- Plan 1: Subscription only
- Plan 2: Subscription and workspace

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`
2. Under `Management`, select `Environment Settings`
3. Click on the subscription name
4. Select `Defender plans` in the left pane
5. Under `Cloud Workload Protection (CWP)`, locate `Server` in the Plan column, ensure Status is set to `On`.

Audit from Azure CLI

Run the following command:

```
az security pricing show -n VirtualMachines --query pricingTier
```

If the tenant is licensed and enabled, the output should indicate `Standard`

Audit from PowerShell
Run the following command:

```
Get-AzSecurityPricing -Name 'VirtualMachines' |Select-Object Name,PricingTier
```

If the tenant is licensed and enabled, the `-PricingTier` parameter will indicate `Standard`

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 4da35fc9-c9e7-4960-aec9-797fe7d9051d **- Name:** 'Azure Defender for servers should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`
2. Under `Management`, select `Environment Settings`
3. Click on the subscription name
4. Click `Defender plans` in the left pane
5. Under `Cloud Workload Protection (CWP)`, locate `Server` in the Plan column, set Status to `On`
6. Select `Save`

Remediate from Azure CLI
Run the following command:

```
az security pricing create -n VirtualMachines --tier 'standard'
```

Remediate from PowerShell
Run the following command:

```
Set-AzSecurityPricing -Name 'VirtualMachines' -PricingTier 'Standard'
```

Default Value:

By default, Microsoft Defender for Servers plan is off.

References:

1. https://learn.microsoft.com/en-us/azure/defender-for-cloud/plan-defender-for-servers
2. https://learn.microsoft.com/en-us/rest/api/defenderforcloud/pricings/list?view=rest-defenderforcloud-2024-01-01&tabs=HTTP

3. https://learn.microsoft.com/en-us/rest/api/defenderforcloud/pricings/update?view=rest-defenderforcloud-2024-01-01&tabs=HTTP
4. https://learn.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing?view=azps-12.2.0
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-endpoint-security#es-1-use-endpoint-detection-and-response-edr

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●
v7	8.1 Utilize Centrally Managed Anti-malware Software Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

3.1.3.2 Ensure that 'Vulnerability assessment for machines' component status is set to 'On' (Manual)

Profile Applicability:

- Level 2

Description:

Enable vulnerability assessment for machines on both Azure and hybrid (Arc enabled) machines.

Rationale:

Vulnerability assessment for machines scans for various security-related configurations and events such as system updates, OS vulnerabilities, and endpoint protection, then produces alerts on threat and vulnerability findings.

Impact:

Microsoft Defender for Servers plan 2 licensing is required, and configuration of Azure Arc introduces complexity beyond this recommendation.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Select a subscription
5. Click on `Settings & monitoring`
6. Ensure that `Vulnerability assessment for machines` is set to `On`

Repeat the above for any additional subscriptions.

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Select a subscription
5. Click on `Settings & Monitoring`
6. Set the `Status` of `Vulnerability assessment for machines` to `On`
7. Click `Continue`

Repeat the above for any additional subscriptions.

Default Value:

By default, `Automatic provisioning of monitoring agent` is set to `Off`.

References:

1. https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-va
2. https://msdn.microsoft.com/en-us/library/mt704062.aspx
3. https://msdn.microsoft.com/en-us/library/mt704063.aspx
4. https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/list
5. https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/create
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-5-perform-vulnerability-assessments

Additional Information:

While this feature is generally available as of publication, it is not yet available for Azure Government tenants.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.3.3 Ensure that 'Endpoint protection' component status is set to 'On' (Manual)

Profile Applicability:

- Level 2

Description:

The Endpoint protection component enables Microsoft Defender for Endpoint (formerly 'Advanced Threat Protection' or 'ATP' or 'WDATP' - see additional info) to communicate with Microsoft Defender for Cloud.

IMPORTANT: When enabling integration between DfE & DfC it needs to be taken into account that this will have some side effects that may be undesirable.

1. For server 2019 & above if defender is installed (default for these server SKUs) this will trigger a deployment of the new unified agent and link to any of the extended configuration in the Defender portal.
2. If the new unified agent is required for server SKUs of Win 2016 or Linux and lower there is additional integration that needs to be switched on and agents need to be aligned.

Rationale:

Microsoft Defender for Endpoint integration brings comprehensive Endpoint Detection and Response (EDR) capabilities within Microsoft Defender for Cloud. This integration helps to spot abnormalities, as well as detect and respond to advanced attacks on endpoints monitored by Microsoft Defender for Cloud.

MDE works only with Standard Tier subscriptions.

Impact:

Endpoint protection requires licensing and is included in these plans:

- Defender for Servers plan 1
- Defender for Servers plan 2

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment Settings`.
4. Click on the subscription name.
5. Click `Settings & monitoring`.

6. Ensure the `Status` for `Endpoint protection` is set to `On`.

Audit from Azure CLI

Ensure the output of the below command is `True`

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<subscriptionID>/providers/Microso
ft.Security/settings?api-version=2021-06-01' | jq '.|.value[] |
select(.name=="WDATP")'|jq '.properties.enabled'
```

Audit from PowerShell

Run the following commands to login and audit this check

```
Connect-AzAccount
Set-AzContext -Subscription <subscriptionID>
Get-AzSecuritySetting | Select-Object name,enabled |where-object {$_.name -eq
"WDATP"}
```

PowerShell Output - Non-Compliant

```
Name  Enabled
----  -------
WDATP    False
```

PowerShell Output - Compliant

```
Name  Enabled
----  -------
WDATP    True
```

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Go to `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment Settings`.
4. Click on the subscription name.
5. Click `Settings & monitoring`.
6. Set the `Status` for `Endpoint protection` to `On`.
7. Click `Continue`.

Remediate from Azure CLI

Use the below command to enable Standard pricing tier for Storage Accounts

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<subscriptionID>/providers/Microso
ft.Security/settings/WDATP?api-version=2021-06-01 -d@"input.json"'
```

Where input.json contains the Request body json data as mentioned below.

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/settings/
WDATP",
  "kind": "DataExportSettings",
  "type": "Microsoft.Security/settings",
  "properties": {
    "enabled": true
  }
}
```

Default Value:

By default, Endpoint protection is `off`.

References:

1. https://docs.microsoft.com/en-in/azure/defender-for-cloud/integration-defender-for-endpoint?tabs=windows
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/settings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/settings/update
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-endpoint-security#es-1-use-endpoint-detection-and-response-edr
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-endpoint-security#es-2-use-modern-anti-malware-software

Additional Information:

IMPORTANT: When enabling integration between DfE & DfC it needs to be taken into account that this will have some side effects that may be undesirable.

1. For server 2019 & above if defender is installed (default for these server SKUs) this will trigger a deployment of the new unified agent and link to any of the extended configuration in the Defender portal.
2. If the new unified agent is required for server SKUs of Win 2016 or Linux and lower there is additional integration that needs to be switched on and agents need to be aligned.

NOTE: "Microsoft Defender for Endpoint (MDE)" was formerly known as "Windows Defender Advanced Threat Protection (WDATP)." There are a number of places (e.g. Azure CLI) where the "WDATP" acronym is still used within Azure.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v8	13.2 Deploy a Host-Based Intrusion Detection Solution Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.3.4 Ensure that 'Agentless scanning for machines' component status is set to 'On' (Manual)

Profile Applicability:

- Level 2

Description:

Using disk snapshots, the agentless scanner scans for installed software, vulnerabilities, and plain text secrets.

Rationale:

The Microsoft Defender for Cloud agentless machine scanner provides threat detection, vulnerability detection, and discovery of sensitive information.

Impact:

Agentless scanning for machines requires licensing and is included in these plans:

- Defender CSPM
- Defender for Servers plan 2

Audit:

Audit from Azure Portal

1. From the Azure Portal `Home` page, select `Microsoft Defender for Cloud`
2. Under `Management` select `Environment Settings`
3. Select a subscription
4. Under `Settings` > `Defender Plans`, click `Settings & monitoring`
5. Under the Component column, locate the row for `Agentless scanning for machines`
6. Ensure that `On` is selected

Repeat the above for any additional subscriptions.

Remediation:

Audit from Azure Portal

1. From the Azure Portal `Home` page, select `Microsoft Defender for Cloud`
2. Under `Management` select `Environment Settings`
3. Select a subscription
4. Under `Settings` > `Defender Plans`, click `Settings & monitoring`
5. Under the Component column, locate the row for `Agentless scanning for machines`

6. Select `On`
7. Click `Continue` in the top left

Repeat the above for any additional subscriptions.

Default Value:

By default, Agentless scanning for machines is `off`.

References:

1. https://learn.microsoft.com/en-us/azure/defender-for-cloud/concept-agentless-data-collection
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification
3. https://learn.microsoft.com/en-us/azure/defender-for-cloud/enable-agentless-scanning-vms

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.3.5 Ensure that 'File Integrity Monitoring' component status is set to 'On' (Manual)

Profile Applicability:

- Level 2

Description:

File Integrity Monitoring (FIM) is a feature that monitors critical system files in Windows or Linux for potential signs of attack or compromise.

Rationale:

FIM provides a detection mechanism for compromised files. When FIM is enabled, critical system files are monitored for changes that might indicate a threat actor is attempting to modify system files for lateral compromise within a host operating system.

Impact:

File Integrity Monitoring requires licensing and is included in these plans:

- Defender for Servers plan 2

Audit:

Audit from Azure Portal

1. From the Azure Portal `Home` page, select `Microsoft Defender for Cloud`
2. Under `Management` select `Environment Settings`
3. Select a subscription
4. Under `Settings` > `Defender Plans`, click `Settings & monitoring`
5. Under the Component column, locate the row for `File Integrity Monitoring`
6. Ensure that `On` is selected

Repeat the above for any additional subscriptions.

Remediation:

Audit from Azure Portal

1. From the Azure Portal `Home` page, select `Microsoft Defender for Cloud`
2. Under `Management` select `Environment Settings`
3. Select a subscription
4. Under `Settings` > `Defender Plans`, click `Settings & monitoring`
5. Under the Component column, locate the row for `File Integrity Monitoring`
6. Select `On`
7. Click `Continue` in the top left

Repeat the above for any additional subscriptions.

Default Value:

By default, File Integrity Monitoring is `Off`.

References:

1. https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-overview
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification
3. https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-enable-defender-endpoint

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.4 Defender Plan: Containers

3.1.4.1 Ensure That Microsoft Defender for Containers Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for Containers enables threat detection for Container Registries including Kubernetes, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud. The following services will be enabled for container instances:

- Defender agent in Azure
- Azure Policy for Kubernetes
- Agentless discovery for Kubernetes
- Agentless container vulnerability assessment

Rationale:

Enabling Microsoft Defender for Container Registries allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Impact:

Turning on Microsoft Defender for Containers incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select `Defender plans`.
5. Ensure the `Status` for `Containers` is set to `On`.

Audit from Azure CLI
Ensure the output of the commands below indicates `Standard` pricing.
For legacy Defender for Container Registries instances:

```
az security pricing show --name "ContainerRegistry" --query pricingTier
```

For new Defender for Containers instances:

```
az security pricing show --name "Containers" --query pricingTier
```

Audit from PowerShell
Ensure the output of the commands below indicates Standard pricing.
For legacy Defender for Container Registries instances:

```
Get-AzSecurityPricing -Name 'ContainerRegistry' | Select-Object
Name,PricingTier
```

For new Defender for Containers instances:

```
Get-AzSecurityPricing -Name 'Containers' | Select-Object Name,PricingTier
```

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 1c988dd6-ade4-430f-a608-2a3e5b0a6d38 **- Name:** 'Microsoft Defender for Containers should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to Microsoft Defender for Cloud.
2. Under Management, select Environment Settings.
3. Click on the subscription name.
4. Select Defender plans.
5. Set Status to On for Containers.
6. Click Save.

Remediate from Azure CLI
(Note: 'ContainerRegistry' has been deprecated and is replaced by 'Containers')
Use the below command to enable Standard pricing tier for Containers.

```
az security pricing create -n 'Containers' --tier 'standard'
```

Remediate from PowerShell
(Note: 'ContainerRegistry' has been deprecated and is replaced by 'Containers')
Use the below command to enable Standard pricing tier for Containers.

```
Set-AzSecurityPricing -Name 'Containers' -PricingTier 'Standard'
```

Default Value:

By default, Microsoft Defender for Containers is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
4. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities
6. https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction?tabs=defender-for-container-arch-aks

Additional Information:

Deprecation of previous product plans 'Container registries' and 'Kubernetes' plans for Microsoft Defender are being deprecated and replaced with 'Containers' or Microsoft Defender for Containers.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.4.2 Ensure that 'Agentless discovery for Kubernetes' component status 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Enable automatic discovery and configuration scanning of the Microsoft Kubernetes clusters.

Rationale:

As with any compute resource, Container environments require hardening and run-time protection to ensure safe operations and detection of threats and vulnerabilities.

Impact:

Agentless discovery for Kubernetes requires licensing and is included in:

- Defender CSPM
- Defender for Containers plans.

Audit:

Audit from Azure Portal

1. From the Azure Portal `Home` page, select `Microsoft Defender for Cloud`
2. Under `Management` select `Environment Settings`
3. Select a subscription
4. Under `Settings` > `Defender Plans`, click `Settings & monitoring`
5. Locate the row for `Agentless discovery for Kubernetes`
6. Ensure that `On` is selected

Repeat the above for any additional subscriptions.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 1c988dd6-ade4-430f-a608-2a3e5b0a6d38 **- Name:** 'Microsoft Defender for Containers should be enabled'

Remediation:

Audit from Azure Portal

1. From the Azure Portal `Home` page, select `Microsoft Defender for Cloud`
2. Under `Management` select `Environment Settings`
3. Select a subscription
4. Under `Settings` > `Defender Plans`, click `Settings & monitoring`
5. Locate the row for `Agentless discovery for Kubernetes`
6. Select `On`
7. Click `Continue` in the top left

Repeat the above for any additional subscriptions.

Default Value:

By default, Microsoft Defender for Containers is `Off`. If Defender for Containers is enabled from the Microsoft Defender for Cloud portal, auto provisioning will be enabled.

References:

1. https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction
2. https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-containers
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/list
6. https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/create
7. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.4.3 Ensure that 'Agentless container vulnerability assessment' component status is 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Enable automatic vulnerability management for images stored in ACR or running in AKS clusters.

Rationale:

Agentless vulnerability scanning will examine container images - whether running or in storage - for vulnerable configurations.

Impact:

Agentless container vulnerability assessment requires licensing and is included in:

- Defender CSPM
- Defender for Containers plans.

Audit:

Audit from Azure Portal

1. From the Azure Portal `Home` page, select `Microsoft Defender for Cloud`
2. Under `Management` select `Environment Settings`
3. Select a subscription
4. Under `Settings` > `Defender Plans`, click `Settings & monitoring`
5. Locate the row for `Agentless container vulnerability assessment`
6. Ensure that `On` is selected

Repeat the above for any additional subscriptions.
Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 1c988dd6-ade4-430f-a608-2a3e5b0a6d38 **- Name:** 'Microsoft Defender for Containers should be enabled'

Remediation:

Audit from Azure Portal

1. From the Azure Portal `Home` page, select `Microsoft Defender for Cloud`
2. Under `Management` select `Environment Settings`
3. Select a subscription
4. Under `Settings` > `Defender Plans`, click `Settings & monitoring`
5. Locate the row for `Agentless container vulnerability assessment`
6. Select `On`
7. Click `Continue` in the top left

Repeat the above for any additional subscriptions.

Default Value:

By default, Microsoft Defender for Containers is `Off`. If Defender for Containers is enabled from the Microsoft Defender for Cloud portal, auto provisioning will be enabled.

References:

1. https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction
2. https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-containers
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/list
6. https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/create
7. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.5 Defender Plan: Storage

3.1.5.1 Ensure That Microsoft Defender for Storage Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for Storage enables threat detection for Storage, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for Storage allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Impact:

Turning on Microsoft Defender for Storage incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Ensure `Status` is set to `On` for `Storage`.

Audit from Azure CLI
Ensure the output of the below command is Standard

```
az security pricing show -n StorageAccounts
```

Audit from PowerShell

```
Get-AzSecurityPricing -Name 'StorageAccounts' | Select-Object
Name,PricingTier
```

Ensure output for `Name PricingTier` is `StorageAccounts Standard`

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 308fbb08-4ab8-4e67-9b29-592e93fb94fa **- Name:** 'Microsoft Defender for Storage (Classic) should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Set `Status` to `On` for `Storage`.
6. Select `Save`.

Remediate from Azure CLI

Ensure the output of the below command is Standard

```
az security pricing create -n StorageAccounts --tier 'standard'
```

Remediate from PowerShell

```
Set-AzSecurityPricing -Name 'StorageAccounts' -PricingTier 'Standard'
```

Default Value:

By default, Microsoft Defender plan is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
4. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.6 Defender Plan: App Service

3.1.6.1 Ensure That Microsoft Defender for App Services Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for App Service enables threat detection for App Service, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for App Service allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Impact:

Turning on Microsoft Defender for App Service incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`
2. Under `Management`, select `Environment Settings`
3. Click on the subscription name
4. Select `Defender plans`
5. Ensure Status is `On` for `App Service`

Audit from Azure CLI
Run the following command:

```
az security pricing show -n AppServices
```

Ensure `-PricingTier` is set to `Standard`

Audit from PowerShell
Run the following command:

```
Get-AzSecurityPricing -Name 'AppServices' |Select-Object Name,PricingTier
```

Ensure the `-PricingTier` is set to `Standard`

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 2913021d-f2fd-4f3d-b958-22354e2bdbcb **- Name:** 'Azure Defender for App Service should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`
2. Under `Management`, select `Environment Settings`
3. Click on the subscription name
4. Select `Defender plans`
5. Set `App Service` Status to `On`
6. Select `Save`

Remediate from Azure CLI
Run the following command:

```
az security pricing create -n Appservices --tier 'standard'
```

Remediate from PowerShell
Run the following command:

```
Set-AzSecurityPricing -Name "AppServices" -PricingTier "Standard"
```

Default Value:

By default, Microsoft Defender plan is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
4. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.7 Defender Plan: Databases

3.1.7.1 Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Microsoft Defender for Azure Cosmos DB scans all incoming network requests for threats to your Azure Cosmos DB resources.

Rationale:

In scanning Azure Cosmos DB requests within a subscription, requests are compared to a heuristic list of potential security threats. These threats could be a result of a security breach within your services, thus scanning for them could prevent a potential security threat from being introduced.

Impact:

Enabling Microsoft Defender for Azure Cosmos DB requires enabling Microsoft Defender for your subscription. Both will incur additional charges.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. On the `Database` row click on `Select types >`.
6. Ensure the toggle switch next to `Azure Cosmos DB` is set to `On`.

Audit from Azure CLI

Ensure the output of the below command is Standard

```
az security pricing show -n CosmosDbs --query pricingTier
```

Audit from PowerShell

```
Get-AzSecurityPricing -Name 'CosmosDbs' | Select-Object Name,PricingTier
```

Ensure output of `-PricingTier` is `Standard`

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** adbe85b5-83e6-4350-ab58-bf3a4f736e5e **- Name:** 'Microsoft Defender for Azure Cosmos DB should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. On the `Database` row click on `Select types >`.
6. Set the toggle switch next to `Azure Cosmos DB` to `On`.
7. Click `Continue`.
8. Click `Save`.

Remediate from Azure CLI

Run the following command:

```
az security pricing create -n 'CosmosDbs' --tier 'standard'
```

Remediate from PowerShell

Use the below command to enable Standard pricing tier for Azure Cosmos DB

```
Set-AzSecurityPricing -Name 'CosmosDbs' -PricingTier 'Standard
```

Default Value:

By default, Microsoft Defender for Azure Cosmos DB is not enabled.

References:

1. https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/
2. https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security
3. https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview
4. https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/cosmos-db-security-baseline
5. https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-enable-database-protections
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.7.2 Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for Open-source relational databases enables threat detection for Open-source relational databases, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for Open-source relational databases allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Impact:

Turning on Microsoft Defender for Open-source relational databases incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Ensure the toggle switch next to `Open-source relational databases` is set to `On`.

Audit from Azure CLI

Run the following command:

```
az security pricing show -n OpenSourceRelationalDatabases --query pricingTier
```

Audit from PowerShell

```
Get-AzSecurityPricing | Where-Object {$_.Name -eq
'OpenSourceRelationalDatabases'} | Select-Object Name, PricingTier
```

Ensure output for `Name PricingTier` is `OpenSourceRelationalDatabases Standard`

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 0a9fbe0d-c5c4-4da8-87d8-f4fd77338835 **- Name:** 'Azure Defender for open-source relational databases should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Set the toggle switch next to `Open-source relational databases` to `On`.
7. Select `Continue`.
8. Select `Save`.

Remediate from Azure CLI

Run the following command:

```
az security pricing create -n 'OpenSourceRelationalDatabases' --tier
'standard'
```

Remediate from PowerShell

Use the below command to enable Standard pricing tier for Open-source relational databases

```
set-azsecuritypricing -name "OpenSourceRelationalDatabases" -pricingtier
"Standard"
```

Default Value:

By default, Microsoft Defender plan is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
3. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-2-monitor-anomalies-and-threats-targeting-sensitive-data

5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.7.3 Ensure That Microsoft Defender for (Managed Instance) Azure SQL Databases Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for Azure SQL Databases enables threat detection for Managed Instance Azure SQL databases, providing threat intelligence, anomaly detection, and behavior analytics in Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for Azure SQL Databases allows for greater defense-in-depth, includes functionality for discovering and classifying sensitive data, surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database.

Impact:

Turning on Microsoft Defender for Azure SQL Databases incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Ensure the toggle switch next to `Azure SQL Databases` is set to `On`.

Audit from Azure CLI

Run the following command:

```
az security pricing show -n SqlServers
```

Ensure `-PricingTier` is set to `Standard`

Audit from PowerShell

Run the following command:

```
Get-AzSecurityPricing -Name 'SqlServers' | Select-Object Name,PricingTier
```

Ensure the `-PricingTier` is set to `Standard`

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL: https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 7fe3b40f-802b-4cdd-8bd4-fd799c948cc2 **- Name:** 'Azure Defender for Azure SQL Database servers should be enabled'
- **Policy ID:** abfb7388-5bf4-4ad7-ba99-2cd2f41cebb9 **- Name:** 'Azure Defender for SQL should be enabled for unprotected SQL Managed Instances'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Set the toggle switch next to `Azure SQL Databases` to `On`.
7. Select `Continue`.
8. Select `Save`.

Remediate from Azure CLI

Run the following command:

```
az security pricing create -n SqlServers --tier 'standard'
```

Remediate from PowerShell

Run the following command:

```
Set-AzSecurityPricing -Name 'SqlServers' -PricingTier 'Standard'
```

Default Value:

By default, Microsoft Defender plan is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
4. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-2-monitor-anomalies-and-threats-targeting-sensitive-data

6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.7.4 Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for SQL servers on machines enables threat detection for SQL servers on machines, providing threat intelligence, anomaly detection, and behavior analytics in Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for SQL servers on machines allows for greater defense-in-depth, functionality for discovering and classifying sensitive data, surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database.

Impact:

Turning on Microsoft Defender for SQL servers on machines incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Ensure the toggle switch next to `SQL servers on machines` is set to `On`.

Audit from Azure CLI

Ensure Defender for SQL is licensed with the following command:

```
az security pricing show -n SqlServerVirtualMachines
```

Ensure the 'PricingTier' is set to 'Standard'

Audit from PowerShell

Run the following command:

```
Get-AzSecurityPricing -Name 'SqlServerVirtualMachines' | Select-Object
Name,PricingTier
```

Ensure the 'PricingTier' is set to 'Standard'

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 6581d072-105e-4418-827f-bd446d56421b **- Name:** 'Azure Defender for SQL servers on machines should be enabled'
- **Policy ID:** abfb4388-5bf4-4ad7-ba82-2cd2f41ceae9 **- Name:** 'Azure Defender for SQL should be enabled for unprotected Azure SQL servers'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Set the toggle switch next to `SQL servers on machines` to `On`.
7. Select `Continue`.
8. Select `Save`.

Remediate from Azure CLI
Run the following command:

```
az security pricing create -n SqlServerVirtualMachines --tier 'standard'
```

Remediate from PowerShell
Run the following command:

```
Set-AzSecurityPricing -Name 'SqlServerVirtualMachines' -PricingTier
'Standard'
```

Default Value:

By default, Microsoft Defender plan is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/defender-for-sql-usage
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
4. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-2-monitor-anomalies-and-threats-targeting-sensitive-data

6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	16.11 Leverage Vetted Modules or Services for Application Security Components Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.8 Defender Plan: Key Vault

3.1.8.1 Ensure That Microsoft Defender for Key Vault Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Turning on Microsoft Defender for Key Vault enables threat detection for Key Vault, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

Rationale:

Enabling Microsoft Defender for Key Vault allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

Impact:

Turning on Microsoft Defender for Key Vault incurs an additional cost per resource.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Ensure `Status` is set to `On` for `Key Vault`.

Audit from Azure CLI

Ensure the output of the below command is Standard

```
az security pricing show -n 'KeyVaults' --query 'pricingTier'
```

Audit from PowerShell

```
Get-AzSecurityPricing -Name 'KeyVaults' | Select-Object Name,PricingTier
```

Ensure output for `PricingTier` is `Standard`

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 0e6763cc-5078-4e64-889d-ff4d9a839047 **- Name:** 'Azure Defender for Key Vault should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Select `On` under `Status` for `Key Vault`.
6. Select `Save`.

Remediate from Azure CLI

Enable Standard pricing tier for Key Vault:

```
az security pricing create -n 'KeyVaults' --tier 'Standard'
```

Remediate from PowerShell

Enable Standard pricing tier for Key Vault:

```
Set-AzSecurityPricing -Name 'KeyVaults' -PricingTier 'Standard'
```

Default Value:

By default, Microsoft Defender plan is off.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
4. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.9 Defender Plan: Resource Manager

3.1.9.1 Ensure That Microsoft Defender for Resource Manager Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Microsoft Defender for Resource Manager scans incoming administrative requests to change your infrastructure from both CLI and the Azure portal.

Rationale:

Scanning resource requests lets you be alerted every time there is suspicious activity in order to prevent a security threat from being introduced.

Impact:

Enabling Microsoft Defender for Resource Manager requires enabling Microsoft Defender for your subscription. Both will incur additional charges.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Ensure `Status` is set to `On` for `Resource Manager`.

Audit from Azure CLI
Ensure the output of the below command is Standard

```
az security pricing show -n 'Arm' --query 'pricingTier'
```

Audit from PowerShell

```
Get-AzSecurityPricing -Name 'Arm' | Select-Object Name,PricingTier
```

Ensure the output of `PricingTier` is `Standard`
Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** c3d20c29-b36d-48fe-808b-99a87530ad99 **- Name:** 'Azure Defender for Resource Manager should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Select `On` under `Status` for `Resource Manager`.
6. Select `Save.

Remediate from Azure CLI

Use the below command to enable Standard pricing tier for Defender for Resource Manager

```
az security pricing create -n 'Arm' --tier 'Standard'
```

Remediate from PowerShell

Use the below command to enable Standard pricing tier for Defender for Resource Manager

```
Set-AzSecurityPricing -Name 'Arm' -PricingTier 'Standard'
```

Default Value:

By default, Microsoft Defender for Resource Manager is not enabled.

References:

1. https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security
2. https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-resource-manager-introduction
3. https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/
4. https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.	●	●	●
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.10 Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed' (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that the latest OS patches for all virtual machines are applied.

Rationale:

Windows and Linux virtual machines should be kept updated to:

- Address a specific bug or flaw
- Improve an OS or application’s general stability
- Fix a security vulnerability

Microsoft Defender for Cloud retrieves a list of available security and critical updates from Windows Update or Windows Server Update Services (WSUS), depending on which service is configured on a Windows VM. The security center also checks for the latest updates in Linux systems. If a VM is missing a system update, the security center will recommend system updates be applied.

Impact:

Running Microsoft Defender for Cloud incurs additional charges for each resource monitored. Please see attached reference for exact charges per hour.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Then the `Recommendations` blade
4. Ensure that there are no recommendations for `Apply system updates`

Alternatively, you can employ your own patch assessment and management tool to periodically assess, report and install the required security patches for your OS.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** bd876905-5b84-4f73-ab2d-2e7a7c4568d9 **- Name:** 'Machines should be configured to periodically check for missing system updates'

Remediation:

Follow Microsoft Azure documentation to apply security patches from the security center. Alternatively, you can employ your own patch assessment and management tool to periodically assess, report, and install the required security patches for your OS.

Default Value:

By default, patches are not automatically deployed.

References:

1. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-6-rapidly-and-automatically-remediate-vulnerabilities
2. https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/
3. https://docs.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.3 Perform Automated Operating System Patch Management Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.	●	●	●
v7	3.4 Deploy Automated Operating System Patch Management Tools Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.	●	●	●

3.1.11 Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

The Microsoft Cloud Security Benchmark (or "MCSB") is an Azure Policy Initiative containing many security policies to evaluate resource configuration against best practice recommendations. If a policy in the MCSB is set with effect type `Disabled`, it is not evaluated and may prevent administrators from being informed of valuable security recommendations.

Rationale:

A security policy defines the desired configuration of resources in your environment and helps ensure compliance with company or regulatory security requirements. The MCSB Policy Initiative a set of security recommendations based on best practices and is associated with every subscription by default. When a policy "Effect" is set to `Audit`, policies in the MCSB ensure that Defender for Cloud evaluates relevant resources for supported recommendations. To ensure that policies within the MCSB are not being missed when the Policy Initiative is evaluated, none of the policies should have an Effect of `Disabled`.

Impact:

Policies within the MCSB default to an effect of `Audit` and will evaluate - but not enforce - policy recommendations. Ensuring these policies are set to `Audit` simply ensures that the evaluation occurs to allow administrators to understand where an improvement may be possible. Administrators will need to determine if the recommendations are relevant and desirable for their environment, then manually take action to resolve the status if desired.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment Settings`.
4. Select the appropriate Subscription.
5. Click on `Security policies` in the left column.
6. Click on `Microsoft cloud security benchmark`.
7. Click `Add Filter` and select `Effect`.
8. Check the `Disabled` box to search for all disabled policies.
9. Click `Apply`.

If no Policies are shown, no Policies are in `Disabled` status and no remediation is necessary.
If any Policies remain in the list, the policy `Effect` should be changed to `Audit`.

Remediation:

Remediate from Azure Portal
Part A - List all disabled policies

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Select the appropriate Subscription
5. Click on `Security policies` in the left column
6. Click on `Microsoft cloud security benchmark`
7. Click `Add Filter` and select `Effect`
8. Check the `Disabled` box to search for all disabled policies
9. Click `Apply`

Part B - Remediate Policy Effect
For each policy that remains in the list:

1. Click the blue ellipses `...` to the right of the policy name
2. Click `Manage effect and parameters`
3. Under Policy effect, select the `Audit` radio button
4. Click `Save`
5. Click `Refresh`

Repeat "Part B - Remediate Policy Effect" until no more policies are listed.

Default Value:

By default, the MCSB policy initiative is associated to all subscriptions and **most** policies will have an effect of `Audit`. Some policies will have a default effect of `Disabled`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-policies
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-transparent-data-encryption
3. https://msdn.microsoft.com/en-us/library/mt704062.aspx
4. https://msdn.microsoft.com/en-us/library/mt704063.aspx
5. https://docs.microsoft.com/en-us/rest/api/policy/policy-assignments/get
6. https://docs.microsoft.com/en-us/rest/api/policy/policy-assignments/create
7. https://docs.microsoft.com/en-in/azure/security-center/tutorial-security-policy

8. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-7-define-and-implement-logging-threat-detection-and-incident-response-strategy

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●
v7	5.5 Implement Automated Configuration Monitoring Systems Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

3.1.12 Ensure That 'All users with the following roles' is set to 'Owner' (Automated)

Profile Applicability:

- Level 1

Description:

Enable security alert emails to subscription owners.

Rationale:

Enabling security alert emails to subscription owners ensures that they receive security alert emails from Microsoft. This ensures that they are aware of any potential security issues and can mitigate the risk in a timely fashion.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Click on the appropriate Management Group, Subscription, or Workspace
5. Click on `Email notifications`
6. Ensure that `All users with the following roles` is set to `Owner`

Audit from Azure CLI
Ensure the command below returns state of `On` and that `Owner` appears in roles.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2020-01-01-preview'| jq '.[] |
select(.name=="default").properties.notificationsByRole'
```

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Click on the appropriate Management Group, Subscription, or Workspace
5. Click on `Email notifications`
6. In the drop down of the `All users with the following roles` field select `Owner`

7. Click Save

Remediate from Azure CLI

Use the below command to set Send email also to subscription owners to On.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts/default1?api-version=2017-08-01-preview -d@"input.json"'
```

Where input.json contains the data below, replacing validEmailAddress with a single email address or multiple comma-separated email addresses:

```
    {
      "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/securityC
ontacts/default1",
      "name": "default1",
      "type": "Microsoft.Security/securityContacts",
      "properties": {
        "email": "<validEmailAddress>",
        "alertNotifications": "On",
        "alertsToAdmins": "On",
       "notificationsByRole": "Owner"
      }
    }
```

Default Value:

By default, Owner is selected

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/security-contacts
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification

Additional Information:

Excluding any entries in the input.json properties block disables the specific setting by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	17.2 Establish and Maintain Contact Information for Reporting Security Incidents Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	●	●	●
v7	19.5 Maintain Contact Information For Reporting Security Incidents Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.	●	●	●

3.1.13 Ensure 'Additional email addresses' is Configured with a Security Contact Email (Automated)

Profile Applicability:

- Level 1

Description:

Microsoft Defender for Cloud emails the subscription owners whenever a high-severity alert is triggered for their subscription. You should provide a security contact email address as an additional email address.

Rationale:

Microsoft Defender for Cloud emails the Subscription Owner to notify them about security alerts. Adding your Security Contact's email address to the 'Additional email addresses' field ensures that your organization's Security Team is included in these alerts. This ensures that the proper people are aware of any potential compromise in order to mitigate the risk in a timely fashion.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment Settings`.
4. Click on the appropriate Management Group, Subscription, or Workspace.
5. Click on `Email notifications`.
6. Ensure that a valid security contact email address is listed in the `Additional email addresses` field.

Audit from Azure CLI

Ensure the output of the below command is not empty and is set with appropriate email ids:

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2020-01-01-preview' | jq '.|.[] |
select(.name=="default")'|jq '.properties.emails'
```

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 4f4f78b8-e367-4b10-a341-d9a4ad5cf1c7 **- Name:** 'Subscriptions should have a contact email address for security issues'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Select `Microsoft Defender for Cloud`.
3. Under `Management`, select `Environment Settings`.
4. Click on the appropriate Management Group, Subscription, or Workspace.
5. Click on `Email notifications`.
6. Enter a valid security contact email address (or multiple addresses separated by commas) in the `Additional email addresses` field.
7. Click `Save`.

Remediate from Azure CLI
Use the below command to set `Security contact emails` to `On`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts/default?api-version=2020-01-01-preview -d@"input.json"'
```

Where `input.json` contains the data below, replacing `validEmailAddress` with a single email address or multiple comma-separated email addresses:

```
    {
      "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/securityC
ontacts/default",
      "name": "default",
      "type": "Microsoft.Security/securityContacts",
      "properties": {
        "email": "<validEmailAddress>",
        "alertNotifications": "On",
        "alertsToAdmins": "On"
      }
    }
```

Default Value:

By default, there are no additional email addresses entered.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/security-contacts
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification

Additional Information:

Excluding any entries in the input.json properties block disables the specific setting by default.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	17.2 Establish and Maintain Contact Information for Reporting Security Incidents Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.	●	●	●
v7	19.5 Maintain Contact Information For Reporting Security Incidents Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.	●	●	●

3.1.14 Ensure That 'Notify about alerts with the following severity' is Set to 'High' (Automated)

Profile Applicability:

- Level 1

Description:

Enables emailing security alerts to the subscription owner or other designated security contact.

Rationale:

Enabling security alert emails ensures that security alert emails are received from Microsoft. This ensures that the right people are aware of any potential security issues and are able to mitigate the risk.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Click on the appropriate Management Group, Subscription, or Workspace
5. Click on `Email notifications`
6. Under `Notification types`, ensure that the `Notify about alerts with the following severity (or higher):` setting is checked and set to `High`

Audit from Azure CLI

Ensure the output of below command is set to `true`, enter your Subscription ID at the $0 between /subscriptions/<$0>/providers.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2020-01-01-preview' | jq '.|.[] |
select(.name=="default")'|jq '.properties.alertNotifications'
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 6e2593d9-add6-4083-9c9b-4b7d2188c899 **- Name:** 'Email notification for high severity alerts should be enabled'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Under `Management`, select `Environment Settings`
4. Click on the appropriate Management Group, Subscription, or Workspace
5. Click on `Email notifications`
6. Under `Notification types`, check the check box next to `Notify about alerts with the following severity (or higher):` and select `High` from the drop down menu
7. Click `Save`

Remediate from Azure CLI

Use the below command to set `Send email notification for high severity alerts` to `On`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<$0>/providers/Microsoft.Security/
securityContacts/default1?api-version=2017-08-01-preview -d@"input.json"'
```

Where `input.json` contains the data below, replacing `validEmailAddress` with a single email address or multiple comma-separated email addresses:

```
       {
      "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/securityC
ontacts/default1",
      "name": "default1",
      "type": "Microsoft.Security/securityContacts",
      "properties": {
        "email": "<validEmailAddress>",
        "alertNotifications": "On",
        "alertsToAdmins": "On"
      }
    }
```

Default Value:

By default, `Notify about alerts with the following severity (or higher):` is set to `High`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list
3. https://docs.microsoft.com/en-us/rest/api/securitycenter/security-contacts

4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-incident-response#ir-2-preparation---setup-incident-notification

Additional Information:

Excluding any entries in the input.json properties block disables the specific setting by default. This recommendation has been updated to reflect recent changes to Microsoft REST APIs for getting and updating security contact information.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.11 Tune Security Event Alerting Thresholds Tune security event alerting thresholds monthly, or more frequently.			●
v7	6.8 Regularly Tune SIEM On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.			●

3.1.15 Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled (Manual)

Profile Applicability:

- Level 2

Description:

An organization's attack surface is the collection of assets with a public network identifier or URI that an external threat actor can see or access from outside your cloud. It is the set of points on the boundary of a system, a system element, system component, or an environment where an attacker can try to enter, cause an effect on, or extract data from, that system, system element, system component, or environment. The larger the attack surface, the harder it is to protect.

This tool can be configured to scan your organization's online infrastructure such as specified domains, hosts, CIDR blocks, and SSL certificates, and store them in an Inventory. Inventory items can be added, reviewed, approved, and removed, and may contain enrichments ("insights") and additional information collected from the tool's different scan engines and open-source intelligence sources.

A Defender EASM workspace will generate an Inventory of publicly exposed assets by crawling and scanning the internet using *Seeds* you provide when setting up the tool. Seeds can be FQDNs, IP CIDR blocks, and WHOIS records.

Defender EASM will generate Insights within 24-48 hours after Seeds are provided, and these insights include vulnerability data (CVEs), ports and protocols, and weak or expired SSL certificates that could be used by an attacker for reconnaisance or exploitation.

Results are classified High/Medium/Low and some of them include proposed mitigations.

Rationale:

This tool can monitor the externally exposed resources of an organization, provide valuable insights, and export these findings in a variety of formats (including CSV) for use in vulnerability management operations and red/purple team exercises.

Impact:

Microsoft Defender EASM workspaces are currently available as Azure Resources with a 30-day free trial period but can quickly accrue significant charges. The costs are calculated daily as (Number of "billable" inventory items) x (item cost per day; approximately: $0.017).

Estimated cost is not provided within the tool, and users are strongly advised to contact their Microsoft sales representative for pricing and set a calendar reminder for the end of the trial period.

For an EASM workspace having an Inventory of 5k-10k billable items (IP addresses, hostnames, SSL certificates, etc) a typical cost might be approximately $85-170 per day or $2500-5000 USD/month at the time of publication.

If the workspace is deleted by the last day of a free trial period, no charges are billed.

Audit:

To view Defender EASM workspaces created for your Subscriptions, search for EASM in the Azure Portal using the search box.

Remediation:

To begin remediation, a Microsoft Defender EASM workspace must be created. The resources and inventory items added to this workspace will depend on your environment.

Default Value:

Microsoft Defender EASM is an optional, paid Azure Resource that must be created and configured inside a Subscription and Resource Group.

References:

1. https://learn.microsoft.com/en-us/azure/external-attack-surface-management/
2. https://learn.microsoft.com/en-us/azure/external-attack-surface-management/deploying-the-defender-easm-azure-resource
3. https://www.microsoft.com/en-us/security/blog/2022/08/02/microsoft-announces-new-solutions-for-threat-intelligence-and-attack-surface-management/

Additional Information:

Microsoft added its Defender for External Attack Surface management (EASM) offering to Azure following its 2022 acquisition of EASM SaaS tool company RiskIQ.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.1.16 [LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On' (Automated)

Profile Applicability:

- Level 2

Description:

[**NOTE:** As of August 1, 2023 customers with an existing subscription to Defender for DNS can continue to use the service, but new subscribers will receive alerts about suspicious DNS activity as part of Defender for Servers P2.]

Microsoft Defender for DNS scans all network traffic exiting from within a subscription.

Rationale:

DNS lookups within a subscription are scanned and compared to a dynamic list of websites that might be potential security threats. These threats could be a result of a security breach within your services, thus scanning for them could prevent a potential security threat from being introduced.

Impact:

Enabling Microsoft Defender for DNS requires enabling Microsoft Defender for your subscription. Both will incur additional charges, with Defender for DNS being a small amount per million queries.

Audit:

Audit from Azure Portal

1. Go to `Microsoft Defender for Cloud`
2. Under `Management`, select `Environment Settings`
3. Click on the subscription name
4. Select the `Defender plans` blade
5. Ensure `Status` is set to `On` for `DNS`.

Audit from Azure CLI

Ensure the output of the below command is Standard

```
az security pricing show -n 'DNS' --query 'PricingTier'
```

Audit from PowerShell

```
Get-AzSecurityPricing --Name 'DNS' | Select-Object Name,PricingTier
```

Ensure output of `PricingTier` is `Standard`

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** bdc59948-5574-49b3-bb91-76b7c986428d **- Name:** 'Azure Defender for DNS should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Under `Management`, select `Environment Settings`.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Select `On` under `Status` for `DNS`.
6. Select `Save`.

Remediate from Azure CLI

Enable Standard pricing tier for DNS:

```
az security pricing create -n 'DNS' --tier 'Standard'
```

Remediate from PowerShell

Enable Standard pricing tier for DNS:

```
Set-AzSecurityPricing -Name 'DNS' -PricingTier 'Standard'
```

Default Value:

By default, Microsoft Defender for DNS is not enabled.

References:

1. https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/
2. https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/dns-security-baseline
3. https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-dns-alerts
4. https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security
5. https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview
6. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-10-ensure-domain-name-system-dns-security
7. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities

Additional Information:

[**NOTE:** As of August 1, 2023 customers with an existing subscription to Defender for DNS can continue to use the service, but new subscribers will receive alerts about suspicious DNS activity as part of Defender for Servers P2.]

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.9 Configure Trusted DNS Servers on Enterprise Assets Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.		●	●
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●
v7	7.6 Log all URL requests Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.		●	●

3.2 Microsoft Defender for IoT

3.2.1 Ensure That Microsoft Defender for IoT Hub Is Set To 'On' (Manual)

Profile Applicability:

- Level 2

Description:

Microsoft Defender for IoT acts as a central security hub for IoT devices within your organization.

Rationale:

IoT devices are very rarely patched and can be potential attack vectors for enterprise networks. Updating their network configuration to use a central security hub allows for detection of these breaches.

Impact:

Enabling Microsoft Defender for IoT will incur additional charges dependent on the level of usage.

Audit:

Audit from Azure Portal

1. Go to `IoT Hub`.
2. Select a `IoT Hub` to validate.
3. Select `Overview` in `Defender for IoT`.
4. The Threat prevention and Threat detection screen will appear, if `Defender for IoT` is Enabled.

Remediation:

Remediate from Azure Portal

1. Go to `IoT Hub`.
2. Select a `IoT Hub` to validate.
3. Select `Overview` in `Defender for IoT`.
4. Click on `Secure your IoT solution`, and complete the onboarding.

Default Value:

By default, Microsoft Defender for IoT is not enabled.

References:

1. https://azure.microsoft.com/en-us/services/iot-defender/#overview

2. https://docs.microsoft.com/en-us/azure/defender-for-iot/
3. https://azure.microsoft.com/en-us/pricing/details/iot-defender/
4. https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/defender-for-iot-security-baseline
5. https://docs.microsoft.com/en-us/cli/azure/iot?view=azure-cli-latest
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-1-enable-threat-detection-capabilities
7. https://learn.microsoft.com/en-us/azure/defender-for-iot/device-builders/quickstart-onboard-iot-hub

Additional Information:

There are additional configurations for Microsoft Defender for IoT that allow for types of deployments called hybrid or local. Both run on your physical infrastructure. These are complicated setups and are primarily outside of the scope of a purely Azure benchmark. Please see the references to consider these options for your organization.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	13.6 Collect Network Traffic Flow Logs Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		●	●
v7	3.1 Run Automated Vulnerability Scanning Tools Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

3.3 Key Vault

This section covers security recommendations to follow for the configuration and use of Azure Key Vault.

3.3.1 Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all Keys in Role Based Access Control (RBAC) Azure Key Vaults have an expiration date set.

Rationale:

Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. The `exp` (expiration date) attribute identifies the expiration date on or after which the key MUST NOT be used for encryption of new data, wrapping of new keys, and signing. By default, keys never expire. It is thus recommended that keys be rotated in the key vault and set an explicit expiration date for all keys to help enforce the key rotation. This ensures that the keys cannot be used beyond their assigned lifetimes.

Impact:

Keys cannot be used beyond their assigned expiration dates respectively. Keys need to be rotated periodically wherever they are used.

Audit:

Audit from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Keys`.
3. In the main pane, ensure that an appropriate `Expiration date` is set for any keys that are `Enabled`.

Audit from Azure CLI

Get a list of all the key vaults in your Azure environment by running the following command:

```
az keyvault list
```

Then for each key vault listed ensure that the output of the below command contains Key ID (kid), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault key list --vault-name <VaultName> --query
'[*].{"kid":kid,"enabled":attributes.enabled,"expires":attributes.expires}'
```

Audit from PowerShell

Retrieve a list of Azure Key vaults:

```
Get-AzKeyVault
```

For each Key vault run the following command to determine which vaults are configured to use RBAC.

```
Get-AzKeyVault -VaultName <VaultName>
```

For each Key vault with the `EnableRbacAuthorizatoin` setting set to `True`, run the following command.

```
Get-AzKeyVaultKey -VaultName <VaultName>
```

Make sure the `Expires` setting is configured with a value as appropriate wherever the `Enabled` setting is set to `True`.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL: https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 152b15f7-8e1f-4c1f-ab71-8c010ba5dbc0 **- Name:** 'Key Vault keys should have an expiration date'

Remediation:

Remediate from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Keys`.
3. In the main pane, ensure that an appropriate `Expiration date` is set for any keys that are `Enabled`.

Remediate from Azure CLI

Update the `Expiration date` for the key using the below command:

```
az keyvault key set-attributes --name <keyName> --vault-name <vaultName> --
expires Y-m-d'T'H:M:S'Z'
```

Note: To view the expiration date on all keys in a Key Vault using Microsoft API, the "List" Key permission is required.

To update the expiration date for the keys:

1. Go to the Key vault, click on Access Control (IAM).
2. Click on Add role assignment and assign the role of Key Vault Crypto Officer to the appropriate user.

Remediate from PowerShell

```
Set-AzKeyVaultKeyAttribute -VaultName <VaultName> -Name <KeyName> -Expires
<DateTime>
```

Default Value:

By default, keys do not expire.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
2. https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-keys
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-6-use-a-secure-key-management-process
4. https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultkeyattribute?view=azps-0.10.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.1 Establish and Maintain a Data Management Process Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

3.3.2 Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults. (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all Keys in Non Role Based Access Control (RBAC) Azure Key Vaults have an expiration date set.

Rationale:

Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. The `exp` (expiration date) attribute identifies the expiration date on or after which the key MUST NOT be used for a cryptographic operation. By default, keys never expire. It is thus recommended that keys be rotated in the key vault and set an explicit expiration date for all keys. This ensures that the keys cannot be used beyond their assigned lifetimes.

Impact:

Keys cannot be used beyond their assigned expiration dates respectively. Keys need to be rotated periodically wherever they are used.

Audit:

Audit from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Keys`.
3. In the main pane, ensure that the status of the key is `Enabled`.
4. For each enabled key, ensure that an appropriate `Expiration date` is set.

Audit from Azure CLI

Get a list of all the key vaults in your Azure environment by running the following command:

```
az keyvault list
```

For each key vault, ensure that the output of the below command contains Key ID (kid), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault key list --vault-name <KEYVAULTNAME> --query
'[*].{"kid":kid,"enabled":attributes.enabled,"expires":attributes.expires}'
```

Audit from PowerShell

Retrieve a list of Azure Key vaults:

```
Get-AzKeyVault
```

For each Key vault, run the following command to determine which vaults are configured to not use RBAC:

```
Get-AzKeyVault -VaultName <Vault Name>
```

For each Key vault with the `EnableRbacAuthorizatoin` setting set to `False` or empty, run the following command.

```
Get-AzKeyVaultKey -VaultName <Vault Name>
```

Make sure the `Expires` setting is configured with a value as appropriate wherever the `Enabled` setting is set to `True`.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 152b15f7-8e1f-4c1f-ab71-8c010ba5dbc0 **- Name:** 'Key Vault keys should have an expiration date'

Remediation:

Remediate from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Keys`.
3. In the main pane, ensure that the status of the key is `Enabled`.
4. For each enabled key, ensure that an appropriate `Expiration date` is set.

Remediate from Azure CLI
Update the `Expiration date` for the key using the below command:

```
az keyvault key set-attributes --name <keyName> --vault-name <vaultName> --
expires Y-m-d'T'H:M:S'Z'
```

Note:
To view the expiration date on all keys in a Key Vault using Microsoft API, the "List" Key permission is required.
To update the expiration date for the keys:

1. Go to Key vault, click on `Access policies`.
2. Click on `Create` and add an access policy with the `Update` permission (in the Key Permissions - Key Management Operations section).

Remediate from PowerShell

```
Set-AzKeyVaultKeyAttribute -VaultName <Vault Name> -Name <Key Name> -Expires
<DateTime>
```

Default Value:

By default, keys do not expire.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
2. https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-keys
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-6-use-a-secure-key-management-process
4. https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultkeyattribute?view=azps-0.10.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.1 Establish and Maintain a Data Management Process Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

3.3.3 Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all Secrets in Role Based Access Control (RBAC) Azure Key Vaults have an expiration date set.

Rationale:

The Azure Key Vault enables users to store and keep secrets within the Microsoft Azure environment. Secrets in the Azure Key Vault are octet sequences with a maximum size of 25k bytes each. The `exp` (expiration date) attribute identifies the expiration date on or after which the secret MUST NOT be used. By default, secrets never expire. It is thus recommended to rotate secrets in the key vault and set an explicit expiration date for all secrets. This ensures that the secrets cannot be used beyond their assigned lifetimes.

Impact:

Secrets cannot be used beyond their assigned expiry date respectively. Secrets need to be rotated periodically wherever they are used.

Audit:

Audit from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Secrets`.
3. In the main pane, ensure that the status of the secret is `Enabled`.
4. For each enabled secret, ensure that an appropriate `Expiration date` is set.

Audit from Azure CLI

Ensure that the output of the below command contains ID (id), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault secret list --vault-name <KEYVAULTNAME> --query
'[*].{"kid":kid,"enabled":attributes.enabled,"expires":attributes.expires}'
```

Audit from PowerShell

Retrieve a list of Key vaults:

```
Get-AzKeyVault
```

For each Key vault, run the following command to determine which vaults are configured to use RBAC:

```
Get-AzKeyVault -VaultName <Vault Name>
```

For each Key vault with the `EnableRbacAuthorization` setting set to `True`, run the following command:

```
Get-AzKeyVaultSecret -VaultName <Vault Name>
```

Make sure the `Expires` setting is configured with a value as appropriate wherever the `Enabled` setting is set to `True`.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 98728c90-32c7-4049-8429-847dc0f4fe37 **- Name:** 'Key Vault secrets should have an expiration date'

Remediation:

Remediate from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Secrets`.
3. In the main pane, ensure that the status of the secret is `Enabled`.
4. For each enabled secret, ensure that an appropriate `Expiration date` is set.

Remediate from Azure CLI
Update the Expiration date for the secret using the below command:

```
az keyvault secret set-attributes --name <secret_name> --vault-name
<vault_name> --expires Y-m-d'T'H:M:S'Z'
```

Note: To view the expiration date on all secrets in a Key Vault using Microsoft API, the `List Secret` permission is required.
To update the expiration date for the secrets:

1. Go to the Key vault, click on `Access Control (IAM)`.
2. Click on `Add role assignment` and assign the role of `Key Vault Secrets Officer` to the appropriate user.

Remediate from PowerShell

```
Set-AzKeyVaultSecretAttribute -VaultName <vault_name> -Name <secret_name> -
Expires <date_time>
```

Default Value:

By default, secrets do not expire.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
2. https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-secrets
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-6-use-a-secure-key-management-process
4. https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultsecretattribute?view=azps-0.10.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.1 Establish and Maintain a Data Management Process Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

3.3.4 Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all Secrets in Non Role Based Access Control (RBAC) Azure Key Vaults have an expiration date set.

Rationale:

The Azure Key Vault enables users to store and keep secrets within the Microsoft Azure environment. Secrets in the Azure Key Vault are octet sequences with a maximum size of 25k bytes each. The `exp` (expiration date) attribute identifies the expiration date on or after which the secret MUST NOT be used. By default, secrets never expire. It is thus recommended to rotate secrets in the key vault and set an explicit expiration date for all secrets. This ensures that the secrets cannot be used beyond their assigned lifetimes.

Impact:

Secrets cannot be used beyond their assigned expiry date respectively. Secrets need to be rotated periodically wherever they are used.

Audit:

Audit from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Secrets`.
3. In the main pane, ensure that the status of the secret is `Enabled`.
4. Set an appropriate `Expiration date` on all secrets.

Audit from Azure CLI

Get a list of all the key vaults in your Azure environment by running the following command:

```
az keyvault list
```

For each key vault, ensure that the output of the below command contains ID (id), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault secret list --vault-name <KEYVALUTNAME> --query
'[*].{"kid":kid,"enabled":attributes.enabled,"expires":attributes.expires}'
```

Audit from PowerShell

Retrieve a list of Key vaults:

```
Get-AzKeyVault
```

For each Key vault run the following command to determine which vaults are configured to use RBAC:

```
Get-AzKeyVault -VaultName <Vault Name>
```

For each Key Vault with the `EnableRbacAuthorization` setting set to `False` or empty, run the following command.

```
Get-AzKeyVaultSecret -VaultName <Vault Name>
```

Make sure the `Expires` setting is configured with a value as appropriate wherever the `Enabled` setting is set to `True`.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 98728c90-32c7-4049-8429-847dc0f4fe37 **- Name:** 'Key Vault secrets should have an expiration date'

Remediation:

Remediate from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, click on `Secrets`.
3. In the main pane, ensure that the status of the secret is `Enabled`.
4. Set an appropriate `Expiration date` on all secrets.

Remediate from Azure CLI

Update the `Expiration date` for the secret using the below command:

```
az keyvault secret set-attributes --name <secret_name> --vault-name
<vault_name> --expires Y-m-d'T'H:M:S'Z'
```

Note:

To view the expiration date on all secrets in a Key Vault using Microsoft API, the `List` Secret permission is required.

To update the expiration date for the secrets:

1. Go to Key vault, click on `Access policies`.
2. Click on `Create` and add an access policy with the `Update` permission (in the Secret Permissions - Secret Management Operations section).

Remediate from PowerShell

For each Key vault with the `EnableRbacAuthorization` setting set to `False` or empty, run the following command.

```
Set-AzKeyVaultSecret -VaultName <vault_name> -Name <secret_name> -Expires
<date_time>
```

Default Value:

By default, secrets do not expire.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-whatis
2. https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-secrets
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-6-use-a-secure-key-management-process
4. https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultsecret?view=azps-7.4.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.1 Establish and Maintain a Data Management Process Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

3.3.5 Ensure the Key Vault is Recoverable (Automated)

Profile Applicability:

- Level 1

Description:

The Key Vault contains object keys, secrets, and certificates. Accidental unavailability of a Key Vault can cause immediate data loss or loss of security functions (authentication, validation, verification, non-repudiation, etc.) supported by the Key Vault objects.

It is recommended the Key Vault be made recoverable by enabling the "Do Not Purge" and "Soft Delete" functions. This is in order to prevent loss of encrypted data, including storage accounts, SQL databases, and/or dependent services provided by Key Vault objects (Keys, Secrets, Certificates) etc. This may happen in the case of accidental deletion by a user or from disruptive activity by a malicious user.

NOTE: In February 2025, Microsoft will enable soft-delete protection on all key vaults, and users will no longer be able to opt out of or turn off soft-delete.

WARNING: A current limitation is that role assignments disappearing when Key Vault is deleted. All role assignments will need to be recreated after recovery.

Rationale:

There could be scenarios where users accidentally run delete/purge commands on Key Vault or an attacker/malicious user deliberately does so in order to cause disruption. Deleting or purging a Key Vault leads to immediate data loss, as keys encrypting data and secrets/certificates allowing access/services will become non-accessible.

There is a Key Vault property that plays a role in permanent unavailability of a Key Vault:

`enablePurgeProtection`: Setting this parameter to "true" for a Key Vault ensures that even if Key Vault is deleted, Key Vault itself or its objects remain recoverable for the next 90 days. Key Vault/objects can either be recovered or purged (permanent deletion) during those 90 days. If no action is taken, the key vault and its objects will subsequently be purged.

Enabling the enablePurgeProtection parameter on Key Vaults ensures that Key Vaults and their objects cannot be deleted/purged permanently.

Impact:

Once purge-protection and soft-delete are enabled for a Key Vault, the action is irreversible.

Audit:

Audit from Azure Portal

1. Go to Key Vaults.
2. For each Key Vault.
3. Click Properties.
4. Ensure the "Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)" is selected for Purge protection option on this key vault`.

Audit from Azure CLI

1. List all Resources of type Key Vaults:

```
az resource list --query "[?type=='Microsoft.KeyVault/vaults']"
```

2. For Every Key Vault ID ensure check parameters enablePurgeProtection is set to true.

```
az resource show --id /subscriptions/xxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/<resourceGroupName>/providers/Microsoft.KeyVault
/vaults/<keyVaultName>
```

Audit from PowerShell
Get all Key Vaults.

```
Get-AzKeyVault
```

For each Key Vault run the following command.

```
Get-AzKeyVault -VaultName <Vault Name>
```

Examine the results of the above command for the EnablePurgeProtection setting. Make sure enablePurgeProtection is set to True.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 0b60c0b2-2dc2-4e1c-b5c9-abbed971de53 **- Name:** 'Key vaults should have deletion protection enabled'
- **Policy ID:** 1e66c121-a66a-4b1f-9b83-0fd99bf0fc2d **- Name:** 'Key vaults should have soft delete enabled'

Remediation:

To enable "Do Not Purge" and "Soft Delete" for a Key Vault:
Remediate from Azure Portal

1. Go to `Key Vaults`.
2. For each Key Vault.
3. Click `Properties`.
4. Ensure the status of Purge protection reads `Enable purge protection (enforce a mandatory retention period for deleted vaults and vault objects)`.
   Note, once enabled you cannot disable it.

Remediate from Azure CLI

```
az resource update --id /subscriptions/xxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/<resourceGroupName>/providers/Microsoft.KeyVault
/vaults/<keyVaultName> --set properties.enablePurgeProtection=true
```

Remediate from PowerShell

```
Update-AzKeyVault -VaultName <vaultName -ResourceGroupName <resourceGroupName
-EnablePurgeProtection
```

Default Value:

When a new Key Vault is created,

- `enableSoftDelete` is enabled by default, and
- `enablePurgeProtection` is disabled by default.

NOTE: In February 2025, Microsoft will enable soft-delete protection on all key vaults, and users will no longer be able to opt out of or turn off soft-delete.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-soft-delete-cli
2. https://learn.microsoft.com/en-us/azure/key-vault/general/soft-delete-overview
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-8-define-and-implement-backup-and-recovery-strategy
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-8-ensure-security-of-key-and-certificate-repository

Additional Information:

When a key is used for SQL server TDE or Encrypting Storage Account, both the features "Do Not Purge" and "Soft Delete" are enabled for the corresponding Key Vault by default by Azure Backend.

WARNING: A current limitation of the soft-delete feature across all Azure services is role assignments disappearing when Key Vault is deleted. All role assignments will need to be recreated after recovery.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 Establish and Maintain a Data Recovery Process Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	10.2 Perform Complete System Backups Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.	●	●	●

3.3.6 Enable Role Based Access Control for Azure Key Vault (Automated)

Profile Applicability:

- Level 2

Description:

The recommended way to access Key Vaults is to use the Azure Role-Based Access Control (RBAC) permissions model.

Azure RBAC is an authorization system built on Azure Resource Manager that provides fine-grained access management of Azure resources. It allows users to manage Key, Secret, and Certificate permissions. It provides one place to manage all permissions across all key vaults.

Rationale:

The new RBAC permissions model for Key Vaults enables a much finer grained access control for key vault secrets, keys, certificates, etc., than the vault access policy. This in turn will permit the use of privileged identity management over these roles, thus securing the key vaults with JIT Access management.

Impact:

Implementation needs to be properly designed from the ground up, as this is a fundamental change to the way key vaults are accessed/managed. Changing permissions to key vaults will result in loss of service as permissions are re-applied. For the least amount of downtime, map your current groups and users to their corresponding permission needs.

Audit:

Audit from Azure Portal

1. From Azure Home open the Portal Menu in the top left corner
2. Select Key Vaults
3. Select a Key Vault to audit
4. Select Access configuration
5. Ensure the Permission Model radio button is set to `Azure role-based access control`

Audit from Azure CLI
Run the following command for each Key Vault in each Resource Group:

```
az keyvault show --resource-group <resource_group> --name <vault_name>
```

Ensure the `enableRbacAuthorization` setting is set to `true` within the output of the above command.

Audit from PowerShell

Run the following PowerShell command:

```
Get-AzKeyVault -Vaultname <vault_name> -ResourceGroupName <resource_group>
```

Ensure the `Enabled For RBAC Authorization` setting is set to `True`

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 12d4fa5e-1f9f-4c21-97a9-b99b3c6611b5 **- Name:** 'Azure Key Vault should use RBAC permission model'

Remediation:

Remediate from Azure Portal

Key Vaults can be configured to use `Azure role-based access control` on creation.
For existing Key Vaults:

1. From Azure Home open the Portal Menu in the top left corner
2. Select `Key Vaults`
3. Select a Key Vault to audit
4. Select `Access configuration`
5. Set the Permission model radio button to `Azure role-based access control`, taking note of the warning message
6. Click `Save`
7. Select `Access Control (IAM)`
8. Select the `Role Assignments` tab
9. Reapply permissions as needed to groups or users

Remediate from Azure CLI

To enable RBAC Authorization for each Key Vault, run the following Azure CLI command:

```
az keyvault update --resource-group <resource_group> --name <vault_name> --
enable-rbac-authorization true
```

Remediate from PowerShell

To enable RBAC authorization on each Key Vault, run the following PowerShell command:

```
Update-AzKeyVault -ResourceGroupName <resource_group> -VaultName <vault_name>
-EnableRbacAuthorization $True
```

Default Value:

The default value for Access control in Key Vaults is Vault Policy.

References:

1. https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-migration#vault-access-policy-to-azure-rbac-migration-steps
2. https://docs.microsoft.com/en-gb/azure/role-based-access-control/role-assignments-portal?tabs=current
3. https://docs.microsoft.com/en-gb/azure/role-based-access-control/overview
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-8-ensure-security-of-key-and-certificate-repository

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	6.8 Define and Maintain Role-Based Access Control Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

3.3.7 Ensure that Private Endpoints are Used for Azure Key Vault (Automated)

Profile Applicability:

- Level 2

Description:

Private endpoints will secure network traffic from Azure Key Vault to the resources requesting secrets and keys.

Rationale:

Private endpoints will keep network requests to Azure Key Vault limited to the endpoints attached to the resources that are whitelisted to communicate with each other. Assigning the Key Vault to a network without an endpoint will allow other resources on that network to view all traffic from the Key Vault to its destination. In spite of the complexity in configuration, this is recommended for high security secrets.

Impact:

Incorrect or poorly-timed changing of network configuration could result in service interruption. There are also additional costs tiers for running a private endpoint per petabyte or more of networking traffic.

Audit:

Audit from Azure Portal

1. From Azure Home open the Portal Menu in the top left.
2. Select Key Vaults.
3. Select a Key Vault to audit.
4. Select `Networking` in the left column.
5. Select `Private endpoint connections` from the top row.
6. View if there is an endpoint attached.

Audit from Azure CLI
Run the following command within a subscription for each Key Vault you wish to audit.

```
az keyvault show --name <keyVaultName>
```

Ensure that `privateEndpointConnections` is not `null`.
Audit from PowerShell
Run the following command within a subscription for each Key Vault you wish to audit.

```
Get-AzPrivateEndpointConnection -PrivateLinkResourceId
'/subscriptions/<subscriptionNumber>/resourceGroups/<resourceGroup>/providers
/Microsoft.KeyVault/vaults/<keyVaultName>/'
```

Ensure that the response contains details of a private endpoint.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** a6abeaec-4d90-4a02-805f-6b26c4d3fbe9 **- Name:** 'Azure Key Vaults should use private link'

Remediation:

Please see the additional information about the requirements needed before starting this remediation procedure.
Remediate from Azure Portal

1. From Azure Home open the Portal Menu in the top left.
2. Select Key Vaults.
3. Select a Key Vault to audit.
4. Select `Networking` in the left column.
5. Select `Private endpoint connections` from the top row.
6. Select `+ Create`.
7. Select the subscription the Key Vault is within, and other desired configuration.
8. Select `Next`.
9. For resource type select `Microsoft.KeyVault/vaults`.
10. Select the Key Vault to associate the Private Endpoint with.
11. Select `Next`.
12. In the `Virtual Networking` field, select the network to assign the Endpoint.
13. Select other configuration options as desired, including an existing or new application security group.
14. Select `Next`.
15. Select the private DNS the Private Endpoints will use.
16. Select `Next`.
17. Optionally add `Tags`.
18. Select `Next : Review + Create`.
19. Review the information and select `Create`. Follow the Audit Procedure to determine if it has successfully applied.
20. Repeat steps 3-19 for each Key Vault.

Remediate from Azure CLI

1. To create an endpoint, run the following command:

```
az network private-endpoint create --resource-group <resourceGroup --vnet-
name <vnetName> --subnet <subnetName> --name <PrivateEndpointName>  --
private-connection-resource-id "/subscriptions/<AZURE SUBSCRIPTION
ID>/resourceGroups/<resourceGroup>/providers/Microsoft.KeyVault/vaults/<keyVa
ultName>" --group-ids vault --connection-name <privateLinkConnectionName> --
location <azureRegion> --manual-request
```

2. To manually approve the endpoint request, run the following command:

```
az keyvault private-endpoint-connection approve --resource-group
<resourceGroup> --vault-name <keyVaultName> –name <privateLinkName>
```

3. Determine the Private Endpoint's IP address to connect the Key Vault to the Private DNS you have previously created:
4. Look for the property networkInterfaces then id; the value must be placed in the variable <privateEndpointNIC> within step 7.

```
az network private-endpoint show -g <resourceGroupName> -n
<privateEndpointName>
```

5. Look for the property networkInterfaces then id; the value must be placed on <privateEndpointNIC> in step 7.

```
az network nic show --ids <privateEndpointName>
```

6. Create a Private DNS record within the DNS Zone you created for the Private Endpoint:

```
az network private-dns record-set a add-record -g <resourcecGroupName> -z
"privatelink.vaultcore.azure.net" -n <keyVaultName> -a <privateEndpointNIC>
```

7. nslookup the private endpoint to determine if the DNS record is correct:

```
nslookup <keyVaultName>.vault.azure.net
nslookup <keyVaultName>.privatelink.vaultcore.azure.n
```

Default Value:

By default, Private Endpoints are not enabled for any services within Azure.

References:

1. https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-overview

2. https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints
3. https://azure.microsoft.com/en-us/pricing/details/private-link/
4. https://docs.microsoft.com/en-us/azure/key-vault/general/private-link-service?tabs=portal
5. https://docs.microsoft.com/en-us/azure/virtual-network/quick-create-portal
6. https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal
7. https://docs.microsoft.com/en-us/azure/bastion/bastion-overview
8. https://docs.microsoft.com/azure/dns/private-dns-getstarted-cli#create-an-additional-dns-record
9. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-8-ensure-security-of-key-and-certificate-repository

Additional Information:

This recommendation assumes that you have created a Resource Group containing a Virtual Network that the services are already associated with and configured private DNS. A Bastion on the virtual network is also required, and the service to which you are connecting must already have a Private Endpoint. For information concerning the installation of these services, please see the attached documentation.

Microsoft's own documentation lists the requirements as: A Key Vault. An Azure virtual network. A subnet in the virtual network. Owner or contributor permissions for both the Key Vault and the virtual network.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	14.1 Segment the Network Based on Sensitivity Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).		●	●

3.3.8 Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services (Automated)

Profile Applicability:

- Level 2

Description:

Automatic Key Rotation is available in Public Preview. The currently supported applications are Key Vault, Managed Disks, and Storage accounts accessing keys within Key Vault. The number of supported applications will incrementally increased.

Rationale:

Once set up, Automatic Private Key Rotation removes the need for manual administration when keys expire at intervals determined by your organization's policy. The recommended key lifetime is 2 years. Your organization should determine its own key expiration policy.

Impact:

There are an additional costs per operation in running the needed applications.

Audit:

Audit from Azure Portal

1. From Azure Portal select the Portal Menu in the top left.
2. Select Key Vaults.
3. Select a Key Vault to audit.
4. Under `Objects` select `Keys`.
5. Select a key to audit.
6. In the top row select `Rotation policy`.
7. Ensure `Enable auto rotation` is set to `Enabled`.
8. Repeat steps 3-7 for each Key Vault and Key.

Audit from Azure CLI
Run the following command:

```
az keyvault key rotation-policy show --vault-name <vaultName> --name
<keyName>
```

Ensure that the response contains a `lifetime action` of `Rotate`.
Audit from PowerShell
Run the following command:

```
Get-AzKeyVaultKeyRotationPolicy -VaultName <vaultName> -Name <keyName>
```

Ensure that the response contains a `lifetime action` of `Rotate`.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** d8cf8476-a2ec-4916-896e-992351803c44 **- Name:** 'Keys should have a rotation policy ensuring that their rotation is scheduled within the specified number of days after creation.'

Remediation:

Note: Azure CLI and Powershell use ISO8601 flags to input timespans. Every timespan input will be in the format P<timespanInISO8601Format>(Y,M,D). The leading P is required with it denoting `period`. The (Y,M,D) are for the duration of Year, Month,and Day respectively. A time frame of 2 years, 2 months, 2 days would be (P2Y2M2D).

Remediate from Azure Portal

1. From Azure Portal select the Portal Menu in the top left.
2. Select Key Vaults.
3. Select a Key Vault to audit.
4. Under `Objects` select `Keys`.
5. Select a key to audit.
6. In the top row select `Rotation policy`.
7. Select an `Expiry time`.
8. Set `Enable auto rotation` to `Enabled`.
9. Set an appropriate `Rotation option` and `Rotation time`.
10. Optionally set the `Notification time`.
11. Select `Save`.
12. Repeat steps 3-11 for each Key Vault and Key.

Remediate from Azure CLI

Run the following command for each key to update its policy to be auto-rotated:

```
az keyvault key rotation-policy update -n <keyName> --vault-name <vaultName>
--value <path/to/policy.json>

Note: It is easiest to supply the policy flags in a .json file. An example
json file would be:

{
  "lifetimeActions": [
    {
      "trigger": {
        "timeAfterCreate": "<timespanInISO8601Format>",
        "timeBeforeExpiry" : null
      },
      "action": {
        "type": "Rotate"
      }
    },
    {
      "trigger": {
        "timeBeforeExpiry" : "<timespanInISO8601Format>"
      },
      "action": {
        "type": "Notify"
      }
    }
  ],
  "attributes": {
    "expiryTime": "<timespanInISO8601Format>"
  }
}
```

Remediate from PowerShell
Run the following command for each key to update its policy:

```
Set-AzKeyVaultKeyRotationPolicy -VaultName test-kv -Name test-key -PolicyPath
rotation_policy.json
```

Note: It is easiest to supply the policy flags in a .json file. An example json file would be:

```
<#
rotation_policy.json
{
    "lifetimeActions": [
      {
        "trigger": {
          "timeAfterCreate": "P<timespanInISO8601Format>M",
          "timeBeforeExpiry": null
        },
        "action": {
          "type": "Rotate"
        }
      },
      {
        "trigger": {
          "timeBeforeExpiry": "P<timespanInISO8601Format>D"
        },
        "action": {
          "type": "Notify"
        }
      }
    ],
    "attributes": {
      "expiryTime": "P<timespanInISO8601Format>Y"
    }
  }
#>
```

Default Value:

By default, Automatic Key Rotation is not enabled.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation
2. https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview#update-the-key-version
3. https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-enable-customer-managed-keys-powershell#set-up-an-azure-key-vault-and-diskencryptionset-optionally-with-automatic-key-rotation
4. https://azure.microsoft.com/en-us/updates/public-preview-automatic-key-rotation-of-customermanaged-keys-for-encrypting-azure-managed-disks/
5. https://docs.microsoft.com/en-us/cli/azure/keyvault/key/rotation-policy?view=azure-cli-latest#az-keyvault-key-rotation-policy-update

6. https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultkeyrotationpolicy?view=azps-8.1.0
7. https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/scalar-data-types/timespan
8. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-6-use-a-secure-key-management-process

Additional Information:

Automatic Key Rotation is in public preview, so any configuration will not change upon full release.

**Note: ** Azure CLI and Powershell use ISO8601 flags to input timespans. Every timespan input will be in the format P<timespanInISO8601Format>(Y,M,D). The leading P is required with it denoting `period`. The (Y,M,D) are for the duration of Year, Month, Day respectively. A time frame of 2 years, 2 months, 2 days would be (P2Y2M2D).

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.1 Establish and Maintain a Data Management Process Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

4 Storage Accounts

This section covers security recommendations to follow to set storage account policies on an Azure Subscription. An Azure storage account provides a unique namespace to store and access Azure Storage data objects.

4.1 Ensure that 'Secure transfer required' is set to 'Enabled' (Automated)

Profile Applicability:

- Level 1

Description:

Enable data encryption in transit.

Rationale:

The secure transfer option enhances the security of a storage account by only allowing requests to the storage account by a secure connection. For example, when calling REST APIs to access storage accounts, the connection must use HTTPS. Any requests using HTTP will be rejected when 'secure transfer required' is enabled. When using the Azure files service, connection without encryption will fail, including scenarios using SMB 2.1, SMB 3.0 without encryption, and some flavors of the Linux SMB client. Because Azure storage doesn’t support HTTPS for custom domain names, this option is not applied when using a custom domain name.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Settings`, click `Configuration`.
3. Ensure that `Secure transfer required` is set to `Enabled`.

Audit from Azure CLI

Use the below command to ensure the `Secure transfer required` is enabled for all the `Storage Accounts` by ensuring the output contains `true` for each of the `Storage Accounts`.

```
az storage account list --query "[*].[name,enableHttpsTrafficOnly]"
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 404c3081-a854-4457-ae30-26a93ef643f9 **- Name:** 'Secure transfer to storage accounts should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to Storage Accounts.
2. For each storage account, under Settings, click Configuration.
3. Set Secure transfer required to Enabled.
4. Click Save.

Remediate from Azure CLI

Use the below command to enable Secure transfer required for a Storage Account

```
az storage account update --name <storageAccountName> --resource-group
<resourceGroupName> --https-only true
```

Default Value:

By default, Secure transfer required is set to Disabled.

References:

1. https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations#encryption-in-transit
2. https://docs.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az_storage_account_list
3. https://docs.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az_storage_account_update
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

4.2 Ensure that ‘Enable Infrastructure Encryption’ for Each Storage Account in Azure Storage is Set to ‘enabled’ (Automated)

Profile Applicability:

- Level 2

Description:

Enabling encryption at the hardware level on top of the default software encryption for Storage Accounts accessing Azure storage solutions.

Rationale:

Azure Storage automatically encrypts all data in a storage account at the network level using 256-bit AES encryption, which is one of the strongest, FIPS 140-2-compliant block ciphers available. Customers who require higher levels of assurance that their data is secure can also enable 256-bit AES encryption at the Azure Storage infrastructure level for double encryption. Double encryption of Azure Storage data protects against a scenario where one of the encryption algorithms or keys may be compromised. Similarly, data is encrypted even before network transmission and in all backups. In this scenario, the additional layer of encryption continues to protect your data. For the most secure implementation of key based encryption, it is recommended to use a Customer Managed asymmetric RSA 2048 Key in Azure Key Vault.

Impact:

The read and write speeds to the storage will be impacted if both default encryption and Infrastructure Encryption are checked, as a secondary form of encryption requires more resource overhead for the cryptography of information. This performance impact should be considered in an analysis for justifying use of the feature in your environment. Customer-managed keys are recommended for the most secure implementation, leading to overhead of key management. The key will also need to be backed up in a secure location, as loss of the key will mean loss of the information in the storage.

Audit:

Audit from Azure Portal

1. From Azure Portal select the portal menu in the top left.
2. Select `Storage Accounts`.
3. Click on each storage account within each resource group you wish to audit.
4. In the overview, under Security, ensure `Infrastructure encryption` is set to `Enabled`.

Audit from Azure CLI

```
az storage blob show \
    --account-name <storage-account> \
    --container-name <container> \
    --name <blob> \
    --query "properties.serverEncrypted"
```

Audit from PowerShell

```
$account = Get-AzStorageAccount -ResourceGroupName <resource-group> `
    -Name <storage-account>
$blob = Get-AzStorageBlob -Context $account.Context `
    -Container <container> `
    -Blob <blob>
$blob.ICloudBlob.Properties.IsServerEncrypted
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 4733ea7b-a883-42fe-8cac-97454c2a9e4a **- Name:** 'Storage accounts should have infrastructure encryption'

Remediation:

Remediate from Azure Portal

1. During Storage Account creation, in the `Encryption` tab, check the box next to `Enable infrastructure encryption`.

Remediate from Azure CLI

Replace the information within <> with appropriate values:

```
az storage account create \
    --name <storage-account> \
    --resource-group <resource-group> \
    --location <location> \
    --sku Standard_RAGRS \
    --kind StorageV2 \
    --require-infrastructure-encryption
```

Remediate from PowerShell
Replace the information within <> with appropriate values:

```
New-AzStorageAccount -ResourceGroupName <resource_group> `
    -AccountName <storage-account> `
    -Location <location> `
    -SkuName "Standard_RAGRS" `
    -Kind StorageV2 `
    -RequireInfrastructureEncryption
```

Enabling Infrastructure Encryption after Storage Account Creation
If infrastructure encryption was not enabled on blob storage creation, there is no ***official*** way to enable it. Please see the additional information section.

Default Value:

By default, Infrastructure Encryption is disabled in blob creation.

References:

1. https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-encryption-status
2. https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption
3. https://docs.microsoft.com/en-us/azure/storage/common/infrastructure-encryption-enable
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-4-enable-data-at-rest-encryption-by-default

Additional Information:

The default service side encryption for Azure Storage is enabled on every block blob, append blob, or page blob that was written to Azure Storage after October 20, 2017. Hardware encryption, however, cannot be enabled on a blob storage after its creation. There are ways to copy all data from a blob storage into another or download and reupload into another blob storage. This could result in data loss and is not recommended.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

4.3 Ensure that 'Enable key rotation reminders' is enabled for each Storage Account (Manual)

Profile Applicability:

- Level 1

Description:

Access Keys authenticate application access requests to data contained in Storage Accounts. A periodic rotation of these keys is recommended to ensure that potentially compromised keys cannot result in a long-term exploitable credential. The "Rotation Reminder" is an automatic reminder feature for a manual procedure.

Rationale:

Reminders such as those generated by this recommendation will help maintain a regular and healthy cadence for activities which improve the overall efficacy of a security program.

Cryptographic key rotation periods will vary depending on your organization's security requirements and the type of data which is being stored in the Storage Account. For example, PCI DSS mandates that cryptographic keys be replaced or rotated 'regularly,' and advises that keys for static data stores be rotated every 'few months.'

For the purposes of this recommendation, 90 days will prescribed for the reminder. Review and adjustment of the 90 day period is recommended, and may even be necessary. Your organization's security requirements should dictate the appropriate setting.

Impact:

This recommendation only creates a periodic reminder to regenerate access keys. Regenerating access keys can affect services in Azure as well as the organization's applications that are dependent on the storage account. All clients that use the access key to access the storage account must be updated to use the new key.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`
2. For each Storage Account, under `Security + networking`, go to `Access keys`
3. If the button `Edit rotation reminder` is displayed, the Storage Account is compliant. Click `Edit rotation reminder` and review the `Remind me every` field for a desirable periodic setting that fits your security program's needs. If the button `Set rotation reminder` is displayed, the Storage Account is not compliant.

Audit from Powershell

```
$rgName = <resource group name for the storage>
$accountName = <storage account name>
$account = Get-AzStorageAccount -ResourceGroupName $rgName -Name $accountName

Write-Output $accountName ->
Write-Output "Expiration Reminder set to:
$($account.KeyPolicy.KeyExpirationPeriodInDays) Days"
Write-Output "Key1 Last Rotated:
$($account.KeyCreationTime.Key1.ToShortDateString())"
Write-Output "Key2 Last Rotated:
$($account.KeyCreationTime.Key2.ToShortDateString())"
```

Key rotation is recommended if the creation date for any key is empty.
If the reminder is set, the period in days will be returned. The recommended period is 90 days.

Remediation:

Remediate from Azure Portal

1. Go to `Storage Accounts`
2. For each Storage Account that is not compliant, under `Security + networking`, go to `Access keys`
3. Click `Set rotation reminder`
4. Check `Enable key rotation reminders`
5. In the `Send reminders` field select `Custom`, then set the `Remind me every` field to `90` and the period drop down to `Days`
6. Click `Save`

Remediate from Powershell

```
$rgName = <resource group name for the storage>
$accountName = <storage account name>
$account = Get-AzStorageAccount -ResourceGroupName $rgName -Name $accountName
if ($account.KeyCreationTime.Key1 -eq $null -or $account.KeyCreationTime.Key2
-eq $null){
        Write-output ("You must regenerate both keys at least once before
setting expiration policy")
} else {
        $account = Set-AzStorageAccount -ResourceGroupName $rgName -Name
$accountName -KeyExpirationPeriodInDay 90
}
$account.KeyPolicy.KeyExpirationPeriodInDays
```

Default Value:

By default, Key rotation reminders is not configured.

References:

1. https://docs.microsoft.com/en-us/azure/storage/common/storage-create-storage-account#regenerate-storage-access-keys

2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-3-manage-application-identities-securely-and-automatically
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-8-restrict-the-exposure-of-credentials-and-secrets
6. https://www.pcidssguide.com/pci-dss-key-rotation-requirements/
7. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v8	13.11 Tune Security Event Alerting Thresholds Tune security event alerting thresholds monthly, or more frequently.			●
v7	6.8 Regularly Tune SIEM On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.			●
v7	11.3 Use Automated Tools to Verify Standard Device Configurations and Detect Changes Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.		●	●

4.4 Ensure that Storage Account Access Keys are Periodically Regenerated (Manual)

Profile Applicability:

- Level 1

Description:

For increased security, regenerate storage account access keys periodically.

Rationale:

When a storage account is created, Azure generates two 512-bit storage access keys which are used for authentication when the storage account is accessed. Rotating these keys periodically ensures that any inadvertent access or exposure does not result from the compromise of these keys.

Cryptographic key rotation periods will vary depending on your organization's security requirements and the type of data which is being stored in the Storage Account. For example, PCI DSS mandates that cryptographic keys be replaced or rotated 'regularly,' and advises that keys for static data stores be rotated every 'few months.'

For the purposes of this recommendation, 90 days will prescribed for the reminder. Review and adjustment of the 90 day period is recommended, and may even be necessary. Your organization's security requirements should dictate the appropriate setting.

Impact:

Regenerating access keys can affect services in Azure as well as the organization's applications that are dependent on the storage account. All clients who use the access key to access the storage account must be updated to use the new key.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`.
2. For each Storage Account, under `Security + networking`, go to `Access keys`.
3. Review the date and days in the `Last rotated` field for **each** key.

If the `Last rotated` field indicates a number or days greater than 90 [or greater than your organization's period of validity], the key should be rotated.

Audit from Azure CLI

1. Get a list of storage accounts

```
az storage account list --subscription <subscription-id>
```

Make a note of `id`, `name` and `resourceGroup`.

2. For every storage account make sure that key is regenerated in past 90 days.

```
az monitor activity-log list --namespace Microsoft.Storage --offset 90d --
query "[?contains(authorization.action, 'regenerateKey')]" --resource-id
<resource id>
```

The output should contain

```
"authorization"/"scope": <your_storage_account> AND "authorization"/"action":
"Microsoft.Storage/storageAccounts/regeneratekey/action" AND
"status"/"localizedValue": "Succeeded" "status"/"Value": "Succeeded"
```

Remediation:

Remediate from Azure Portal

1. Go to `Storage Accounts`.
2. For each Storage Account with outdated keys, under `Security + networking`, go to `Access keys`.
3. Click `Rotate key` next to the outdated key, then click `Yes` to the prompt confirming that you want to regenerate the access key.

After Azure regenerates the Access Key, you can confirm that `Access keys` reflects a `Last rotated` date of `(0 days ago)`.

Default Value:

By default, access keys are not regenerated periodically.

References:

1. https://docs.microsoft.com/en-us/azure/storage/common/storage-create-storage-account#regenerate-storage-access-keys
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-1-separate-and-limit-highly-privilegedadministrative-users
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-2-protect-identity-and-authentication-systems
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy
5. https://www.pcidssguide.com/pci-dss-key-rotation-requirements/
6. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	●	●	●
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

4.5 Ensure that Shared Access Signature Tokens Expire Within an Hour (Manual)

Profile Applicability:

- Level 1

Description:

Expire shared access signature tokens within an hour.

Rationale:

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. A shared access signature can be provided to clients who should not be trusted with the storage account key but for whom it may be necessary to delegate access to certain storage account resources. Providing a shared access signature URI to these clients allows them access to a resource for a specified period of time. This time should be set as low as possible and preferably no longer than an hour.

Audit:

Currently, SAS token expiration times cannot be audited. Until Microsoft makes token expiration time a setting rather than a token creation parameter, this recommendation would require a manual verification.

Remediation:

When generating shared access signature tokens, use start and end time such that it falls within an hour.
Remediate from Azure Portal

1. Go to Storage Accounts
2. For each storage account where a shared access signature is required, under `Security + networking`, go to `Shared access signature`
3. Select the appropriate `Allowed resource types`
4. Set the `Start and expiry date/time` to be within one hour
5. Click `Generate SAS and connection string`

Default Value:

By default, expiration for shared access signature is set to 8 hours.

References:

1. https://docs.microsoft.com/en-us/rest/api/storageservices/delegating-access-with-a-shared-access-signature
2. https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.2 Establish an Access Revoking Process Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.	●	●	●
v7	16.7 Establish Process for Revoking Access Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.		●	●

4.6 Ensure that 'Public Network Access' is 'Disabled' for storage accounts (Automated)

Profile Applicability:

- Level 1

Description:

Disallowing public network access for a storage account overrides the public access settings for individual containers in that storage account for Azure Resource Manager Deployment Model storage accounts. Azure Storage accounts that use the classic deployment model will be retired on August 31, 2024.

Rationale:

The default network configuration for a storage account permits a user with appropriate permissions to configure public network access to containers and blobs in a storage account. Keep in mind that public access to a container is always turned off by default and must be explicitly configured to permit anonymous requests. It grants read-only access to these resources without sharing the account key, and without requiring a shared access signature. It is recommended not to provide public network access to storage accounts until, and unless, it is strongly desired. A shared access signature token or Azure AD RBAC should be used for providing controlled and timed access to blob containers.

Impact:

Access will have to be managed using shared access signatures or via Azure AD RBAC.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under the `Security + networking` section, click `Networking`.
3. Ensure the `Public network access` setting is set to `Disabled`.

Audit from Azure CLI
Ensure `publicNetworkAccess` is `Disabled`

```
az storage account show --name <storage-account> --resource-group <resource-group> --query "{publicNetworkAccess:publicNetworkAccess}"
```

Audit from PowerShell
For each Storage Account, ensure `PublicNetworkAccess` is `Disabled`

```
Get-AzStorageAccount -Name <storage account name> -ResourceGroupName
<resource group name> |select PublicNetworkAccess
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** b2982f36-99f2-4db5-8eff-283140c09693 **- Name:** 'Storage accounts should disable public network access'

Remediation:

Remediate from Azure Portal

First, follow Microsoft documentation and create shared access signature tokens for your blob containers. Then,

1. Go to `Storage Accounts`.
2. For each storage account, under the `Security + networking` section, click `Networking`.
3. Set `Public network access` to `Disabled`.
4. Click `Save`.

Remediate from Azure CLI

Set 'Public Network Access' to `Disabled` on the storage account

```
az storage account update --name <storage-account> --resource-group
<resource-group> --public-network-access Disabled
```

Remediate from PowerShell

For each Storage Account, run the following to set the `PublicNetworkAccess` setting to `Disabled`

```
Set-AzStorageAccount -ResourceGroupName <resource group name> -Name <storage
account name> -PublicNetworkAccess Disabled
```

Default Value:

By default, `Public Network Access` is set to `Enabled from all networks` for the Storage Account.

References:

1. https://docs.microsoft.com/en-us/azure/storage/blobs/storage-manage-access-to-resources
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy

3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls
4. https://docs.microsoft.com/en-us/azure/storage/blobs/assign-azure-role-data-access
5. https://learn.microsoft.com/en-us/azure/storage/common/storage-network-security?tabs=azure-portal

Additional Information:

For classic storage accounts (to be retired on August 31, 2024), each container in the account must be configured to block anonymous access. Either configure all containers or to configure at the storage account level, migrate to the Azure Resource Manager deployment model.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

4.7 Ensure Default Network Access Rule for Storage Accounts is Set to Deny (Automated)

Profile Applicability:

- Level 1

Description:

Restricting default network access helps to provide a new layer of security, since storage accounts accept connections from clients on any network. To limit access to selected networks, the default action must be changed.

Rationale:

Storage accounts should be configured to deny access to traffic from all networks (including internet traffic). Access can be granted to traffic from specific Azure Virtual networks, allowing a secure network boundary for specific applications to be built. Access can also be granted to public internet IP address ranges to enable connections from specific internet or on-premises clients. When network rules are configured, only applications from allowed networks can access a storage account. When calling from an allowed network, applications continue to require proper authorization (a valid access key or SAS token) to access the storage account.

Impact:

All allowed networks will need to be whitelisted on each specific network, creating administrative overhead. This may result in loss of network connectivity, so do not turn on for critical resources during business hours.

Audit:

Audit from Azure Portal

1. Go to Storage Accounts.
2. For each storage account, under `Security + networking`, click `Networking`.
3. Click the `Firewalls and virtual networks` heading.
4. Ensure that `Public network access` is not set to `Enabled from all networks`.

Audit from Azure CLI
Ensure `defaultAction` is not set to `Allow`.

```
    az storage account list --query '[*].networkRuleSet'
```

Audit from PowerShell

```
Connect-AzAccount
Set-AzContext -Subscription <subscription ID>
Get-AzStorageAccountNetworkRuleset -ResourceGroupName <resource group> -Name
<storage account name> |Select-Object DefaultAction
```

PowerShell Result - Non-Compliant

```
DefaultAction        : Allow
```

PowerShell Result - Compliant

```
DefaultAction        : Deny
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 34c877ad-507e-4c82-993e-3452a6e0ad3c **- Name:** 'Storage accounts should restrict network access'
- **Policy ID:** 2a1a9cdf-e04d-429a-8416-3bfb72a1b26f **- Name:** 'Storage accounts should restrict network access using virtual network rules'

Remediation:

Remediate from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Security + networking`, click `Networking`.
3. Click the `Firewalls and virtual networks` heading.
4. Set `Public network access` to `Enabled from selected virtual networks and IP addresses`.
5. Add rules to allow traffic from specific networks and IP addresses.
6. Click `Save`.

Remediate from Azure CLI

Use the below command to update `default-action` to `Deny`.

```
    az storage account update --name <StorageAccountName> --resource-group
<resourceGroupName> --default-action Deny
```

Default Value:

By default, Storage Accounts will accept connections from clients on any network.

References:

1. https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

4.8 Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access (Automated)

Profile Applicability:

- Level 2

Description:

NOTE: This recommendation assumes that the `Public network access` parameter is set to `Enabled from selected virtual networks and IP addresses`. Please ensure the prerequisite recommendation has been implemented before proceeding:

- Ensure Default Network Access Rule for Storage Accounts is Set to Deny

Some Azure 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 Azure services to bypass the network rules. These services will then use strong authentication to access the storage account. If the `Allow Azure services on the trusted services list to access this storage account` exception is enabled, the following services are granted access to the storage account: Azure Backup, Azure Data Box, Azure DevTest Labs, Azure Event Grid, Azure Event Hubs, Azure File Sync, Azure HDInsight, Azure Import/Export, Azure Monitor, Azure Networking Services, and Azure Site Recovery (when registered in the subscription).

Rationale:

Turning on firewall rules for a storage account will block access to incoming requests for data, including from other Azure services. We can re-enable this functionality by allowing access to `trusted Azure services` through networking exceptions.

Impact:

This creates authentication credentials for services that need access to storage resources so that services will no longer need to communicate via network request. There may be a temporary loss of communication as you set each Storage Account. It is recommended to not do this on mission-critical resources during business hours.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Security + networking`, click `Networking`.
3. Click on the `Firewalls and virtual networks` heading.

4. Under `Exceptions`, ensure that `Allow Azure services on the trusted services list to access this storage account` is checked.

Audit from Azure CLI

Ensure `bypass` contains `AzureServices`

```
az storage account list --query '[*].networkRuleSet'
```

Audit from PowerShell

```
Connect-AzAccount
Set-AzContext -Subscription <subscription ID>
Get-AzStorageAccountNetworkRuleset -ResourceGroupName <resource group> -Name
<storage account name> |Select-Object Bypass
```

If the response from the above command is `None`, the storage account configuration is out of compliance with this check. If the response is `AzureServices`, the storage account configuration is in compliance with this check.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** c9d007d0-c057-4772-b18c-01e546713bcd **- Name:** 'Storage accounts should allow access from trusted Microsoft services'

Remediation:

Remediate from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Security + networking`, click `Networking`.
3. Click on the `Firewalls and virtual networks` heading.
4. Under `Exceptions`, check the box next to `Allow Azure services on the trusted services list to access this storage account`.
5. Click `Save`.

Remediate from Azure CLI

Use the below command to update `bypass` to `Azure services`.

```
az storage account update --name <StorageAccountName> --resource-group
<resourceGroupName> --bypass AzureServices
```

Default Value:

By default, Storage Accounts will accept connections from clients on any network.

References:

1. https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	13.5 Manage Access Control for Remote Assets Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.		●	●
v7	13.3 Monitor and Block Unauthorized Network Traffic Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

4.9 Ensure Private Endpoints are used to access Storage Accounts (Automated)

Profile Applicability:

- Level 2

Description:

Use private endpoints for your Azure Storage accounts to allow clients and services to securely access data located over a network via an encrypted Private Link. To do this, the private endpoint uses an IP address from the VNet for each service. Network traffic between disparate services securely traverses encrypted over the VNet. This VNet can also link addressing space, extending your network and accessing resources on it. Similarly, it can be a tunnel through public networks to connect remote infrastructures together. This creates further security through segmenting network traffic and preventing outside sources from accessing it.

Rationale:

Securing traffic between services through encryption protects the data from easy interception and reading.

Impact:

A Private Endpoint costs approximately US$7.30 per month. If an Azure Virtual Network is not implemented correctly, this may result in the loss of critical network traffic.

Audit:

Audit from Azure Portal

1. Open the `Storage Accounts` blade.
2. For each listed Storage Account, perform the following check:
3. Under the `Security + networking` heading, click on `Networking`.
4. Click on the `Private endpoint connections` tab at the top of the networking window.
5. Ensure that for each VNet that the Storage Account must be accessed from, a unique Private Endpoint is deployed and the `Connection state` for each Private Endpoint is `Approved`.

Repeat the procedure for each Storage Account.

Audit from PowerShell

```
$storageAccount = Get-AzStorageAccount -ResourceGroup '<ResourceGroupName>' -
Name '<storageaccountname>'


Get-AzPrivateEndpoint -ResourceGroup '<ResourceGroupName>'|Where-Object
{$_.PrivateLinkServiceConnectionsText -match $storageAccount.id}
```

If the results of the second command returns information, the Storage Account is using a Private Endpoint and complies with this Benchmark, otherwise if the results of the second command are empty, the Storage Account generates a finding.

Audit from Azure CLI

```
az storage account show --name '<storage account name>' --query
"privateEndpointConnections[0].id"
```

If the above command returns data, the Storage Account complies with this Benchmark, otherwise if the results are empty, the Storage Account generates a finding.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 6edd7eda-6dd8-40f7-810d-67160c639cd9 **- Name:** 'Storage accounts should use private link'

Remediation:

Remediate from Azure Portal

1. Open the `Storage Accounts` blade
2. For each listed Storage Account, perform the following:
3. Under the `Security + networking` heading, click on `Networking`
4. Click on the `Private endpoint connections` tab at the top of the networking window
5. Click the `+ Private endpoint` button
6. In the `1 - Basics` tab/step:
    - `Enter a name` that will be easily recognizable as associated with the Storage Account (*Note*: The "Network Interface Name" will be automatically completed, but you can customize it if needed.)
    - Ensure that the `Region` matches the region of the Storage Account
    - Click `Next`

7. In the `2 - Resource` tab/step:
    - Select the `target sub-resource` based on what type of storage resource is being made available
    - Click `Next`
8. In the `3 - Virtual Network` tab/step:
    - Select the `Virtual network` that your Storage Account will be connecting to
    - Select the `Subnet` that your Storage Account will be connecting to
    - (Optional) Select other network settings as appropriate for your environment
    - Click `Next`
9. In the `4 - DNS` tab/step:
    - (Optional) Select other DNS settings as appropriate for your environment
    - Click `Next`
10. In the `5 - Tags` tab/step:
    - (Optional) Set any tags that are relevant to your organization
    - Click `Next`
11. In the `6 - Review + create` tab/step:
    - A validation attempt will be made and after a few moments it should indicate `Validation Passed` - if it does not pass, double-check your settings before beginning more in depth troubleshooting.
    - If validation has passed, click `Create` then wait for a few minutes for the scripted deployment to complete.

Repeat the above procedure for each Private Endpoint required within every Storage Account.

Remediate from PowerShell

```
$storageAccount = Get-AzStorageAccount -ResourceGroupName
'<ResourceGroupName>' -Name '<storageaccountname>'


$privateEndpointConnection = @{
                                Name = 'connectionName'
                                PrivateLinkServiceId = $storageAccount.Id
                                GroupID =
"blob|blob_secondary|file|file_secondary|table|table_secondary|queue|queue_se
condary|web|web_secondary|dfs|dfs_secondary"
}


$privateLinkServiceConnection = New-AzPrivateLinkServiceConnection
@privateEndpointConnection


$virtualNetDetails = Get-AzVirtualNetwork -ResourceGroupName
'<ResourceGroupName>' -Name '<name>'


$privateEndpoint = @{
                    ResourceGroupName = '<ResourceGroupName>'
                    Name = '<PrivateEndpointName>'
                    Location = '<location>'
                    Subnet = $virtualNetDetails.Subnets[0]
                    PrivateLinkServiceConnection =
$privateLinkServiceConnection
}

New-AzPrivateEndpoint @privateEndpoint
```

Remediate from Azure CLI

```
az network private-endpoint create --resource-group <ResourceGroupName --
location <location> --name <private endpoint name> --vnet-name <VNET Name> --
subnet <subnet name> --private-connection-resource-id <storage account ID> --
connection-name <private link service connection name> --group-id
<blob|blob_secondary|file|file_secondary|table|table_secondary|queue|queue_se
condary|web|web_secondary|dfs|dfs_secondary>
```

Default Value:

By default, Private Endpoints are not created for Storage Accounts.

References:

1. https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints
2. https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview
3. https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-portal
4. https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-cli?tabs=dynamic-ip

5. https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-powershell?tabs=dynamic-ip
6. https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal
7. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls

Additional Information:

A NAT gateway is the recommended solution for outbound internet access.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	14.1 Segment the Network Based on Sensitivity Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).		●	●

4.10 Ensure Soft Delete is Enabled for Azure Containers and Blob Storage (Automated)

Profile Applicability:

- Level 1

Description:

The Azure Storage blobs contain data like ePHI or Financial, which can be secret or personal. Data that is erroneously modified or deleted by an application or other storage account user will cause data loss or unavailability.

It is recommended that both Azure Containers with attached Blob Storage and standalone containers with Blob Storage be made recoverable by enabling the **soft delete** configuration. This is to save and recover data when blobs or blob snapshots are deleted.

Rationale:

Containers and Blob Storage data can be incorrectly deleted. An attacker/malicious user may do this deliberately in order to cause disruption. Deleting an Azure Storage blob causes immediate data loss. Enabling this configuration for Azure storage ensures that even if blobs/data were deleted from the storage account, Blobs/data objects are recoverable for a particular time which is set in the "Retention policies," ranging from 7 days to 365 days.

Impact:

Additional storage costs may be incurred as snapshots are retained.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`.
2. For each Storage Account, under `Data management`, go to `Data protection`.
3. Ensure that `Enable soft delete for blobs` is checked.
4. Ensure that `Enable soft delete for containers` is checked.
5. Ensure that the retention period for both is a sufficient length for your organization.

Audit from Azure CLI
Blob Storage: Ensure that the output of the below command contains enabled status as true and days is not empty or null

```
az storage blob service-properties delete-policy show
    --account-name <storageAccount>
    --account-key <accountkey>
```

Azure Containers: Ensure that within `containerDeleteRetentionPolicy`, the `enabled` property is set to `true`.

```
az storage account blob-service-properties show
    --account-name <storageAccount>
    --resource-group <resourceGroup>
```

Remediation:

Remediate from Azure Portal

1. Go to `Storage Accounts`.
2. For each Storage Account, under `Data management`, go to `Data protection`.
3. Check the box next to `Enable soft delete for blobs`.
4. Check the box next to `Enable soft delete for containers`.
5. Set the retention period for both to a sufficient length for your organization.
6. Click `Save`.

Remediate from Azure CLI

Update blob storage retention days in below command

```
az storage blob service-properties delete-policy update --days-retained
<RetentionDaysValue> --account-name <StorageAccountName> --account-key
<AccountKey> --enable true
```

Update container retention with the below command

```
az storage account blob-service-properties update
    --enable-container-delete-retention true
    --container-delete-retention-days <days>
    --account-name <storageAccount>
    --resource-group <resourceGroup>
```

Default Value:

Soft delete for containers and blob storage is **enabled** by default on storage accounts created via the Azure Portal, and **disabled** by default on storage accounts created via Azure CLI or PowerShell.

References:

1. https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-soft-delete
2. https://docs.microsoft.com/en-us/azure/storage/blobs/soft-delete-container-overview
3. https://docs.microsoft.com/en-us/azure/storage/blobs/soft-delete-container-enable?tabs=azure-portal

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	11.1 Establish and Maintain a Data Recovery Process Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	10.4 Ensure Protection of Backups Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.	●	●	●

4.11 Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK) (Manual)

Profile Applicability:

- Level 2

Description:

Enable sensitive data encryption at rest using Customer Managed Keys (CMK) rather than Microsoft Managed keys.

Rationale:

By default, data in the storage account is encrypted using Microsoft Managed Keys at rest. All Azure Storage resources are encrypted, including blobs, disks, files, queues, and tables. All object metadata is also encrypted. If you want to control and manage this encryption key yourself, however, you can specify a customer-managed key. That key is used to protect and control access to the key that encrypts your data. You can also choose to automatically update the key version used for Azure Storage encryption whenever a new version is available in the associated Key Vault.

While it is possible to automate the assessment of this recommendation, the assessment status for this recommendation remains 'Manual.' This is because the recommendation pertains to storage accounts that store critical data and is therefore not applicable to all storage accounts.

Impact:

If the key expires by setting the 'activation date' and 'expiration date', the user must rotate the key manually.

Using Customer Managed Keys may also incur additional man-hour requirements to create, store, manage, and protect the keys as needed.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`
2. For each storage account, under `Security + networking`, go to `Encryption`
3. Ensure that `Encryption type` is set to `Customer-managed keys`

Audit from PowerShell

```
Connect-AzAccount
Set-AzContext -Subscription <subscription id>
Get-AzStorageAccount |Select-Object -ExpandProperty Encryption
```

PowerShell Results - Non-Compliant

```
...
KeySource                        : Microsoft.Storage
...
```

PowerShell Results - Compliant

```
...
KeySource                        : Microsoft.Keyvault
...
```

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 6fac406b-40ca-413b-bf8e-0bf964659c25 **- Name:** 'Storage accounts should use customer-managed key for encryption'

Remediation:

Remediate from Azure Portal

1. Go to `Storage Accounts`
2. For each storage account, under `Security + networking`, go to `Encryption`
3. Set `Encryption type` to `Customer-managed keys`
4. Select an encryption key or enter a key URI
5. Click `Save`

Default Value:

By default, Encryption type is set to Microsoft Managed Keys.

References:

1. https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption
2. https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices#protect-data-at-rest
3. https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption#azure-storage-encryption-versus-disk-encryption
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

4.12 Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests (Automated)

Profile Applicability:

- Level 2

Description:

The Storage Queue service stores messages that may be read by any client who has access to the storage account. A queue can contain an unlimited number of messages, each of which can be up to 64KB in size using version 2011-08-18 or newer. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the queues. Storage Logging log entries contain the following information about individual requests: Timing information such as start time, end-to-end latency, and server latency, authentication details, concurrency information, and the sizes of the request and response messages.

Rationale:

Storage Analytics logs contain detailed information about successful and failed requests to a storage service. This information can be used to monitor individual requests and to diagnose issues with a storage service. Requests are logged on a best-effort basis.

Storage Analytics logging is not enabled by default for your storage account.

Impact:

Enabling this setting can have a high impact on the cost of the log analytics service and data storage used by logging more data per each request. Do not enable this without determining your need for this level of logging, and do not forget to check in on data usage and projected cost. Some users have seen their logging costs increase from $10 per month to $10,000 per month.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Monitoring`, click `Diagnostics settings`.
3. Select the `queue` tab indented below the storage account.
4. Ensure that at least one diagnostic setting is listed.
5. Click `Edit setting` on a diagnostic setting.
6. Ensure that at least one diagnostic setting has `StorageRead`, `StorageWrite`, and `StorageDelete` options selected under the `Logs` section and that they are sent to an appropriate destination.

Audit from Azure CLI
Ensure the below command's output contains properties `delete`, `read` and `write` set to `true`.

```
az storage logging show --services q --account-name <storageAccountName>
```

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 7bd000e3-37c7-4928-9f31-86c4b77c5c45 **- Name:** 'Configure diagnostic settings for Queue Services to Log Analytics workspace'

Remediation:

Remediate from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Monitoring`, click `Diagnostics settings`.
3. Select the `queue` tab indented below the storage account.
4. To create a new diagnostic setting, click `+ Add diagnostic setting`. To update an existing diagnostic setting, click `Edit setting` on the diagnostic setting.
5. Check the boxes next to `StorageRead`, `StorageWrite`, and `StorageDelete`.
6. Select an appropriate destination.
7. Click `Save`.

Remediate from Azure CLI
Use the below command to enable the Storage Logging for Queue service.

```
az storage logging update --account-name <storageAccountName> --account-key
<storageAccountKey> --services q --log rwd --retention 90
```

Default Value:

By default storage account queue services are not logged.

References:

1. https://docs.microsoft.com/en-us/rest/api/storageservices/about-storage-analytics-logging
2. https://docs.microsoft.com/en-us/cli/azure/storage/logging?view=azure-cli-latest
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-4-enable-network-logging-for-security-investigation
4. https://docs.microsoft.com/en-us/azure/storage/queues/monitor-queue-storage?tabs=azure-portal

Additional Information:

We cannot practically generalize detailed audit log requirements for every queue due to their nature and intent. This recommendation may be applicable to storage account queue services where security is paramount.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.13 Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests (Automated)

Profile Applicability:

- Level 2

Description:

The Storage Blob service provides scalable, cost-efficient object storage in the cloud. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the blobs. Storage Logging log entries contain the following information about individual requests: timing information such as start time, end-to-end latency, and server latency; authentication details; concurrency information; and the sizes of the request and response messages.

Rationale:

Storage Analytics logs contain detailed information about successful and failed requests to a storage service. This information can be used to monitor each individual request to a storage service for increased security or diagnostics. Requests are logged on a best-effort basis.

Storage Analytics logging is not enabled by default for your storage account.

Impact:

Being a level 2, enabling this setting can have a high impact on the cost of data storage used for logging more data per each request. Do not enable this without determining your need for this level of logging or forget to check in on data usage and projected cost.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Monitoring`, click `Diagnostics settings`.
3. Select the `blob` tab indented below the storage account.
4. Ensure that at least one diagnostic setting is listed.
5. Click `Edit setting` on a diagnostic setting.
6. Ensure that at least one diagnostic setting has `StorageRead`, `StorageWrite`, and `StorageDelete` options selected under the `Logs` section and that they are sent to an appropriate destination.
   Audit from Azure CLI

Ensure the below command's output contains properties delete, read and write set to true.

```
az storage logging show --services b --account-name <storageAccountName>
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** b4fe1a3b-0715-4c6c-a5ea-ffc33cf823cb **- Name:** 'Configure diagnostic settings for Blob Services to Log Analytics workspace'

Remediation:

Remediate from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Monitoring`, click `Diagnostics settings`.
3. Select the `blob` tab indented below the storage account.
4. To create a new diagnostic setting, click `+ Add diagnostic setting`. To update an existing diagnostic setting, click `Edit setting` on the diagnostic setting.
5. Check the boxes next to `StorageRead`, `StorageWrite`, and `StorageDelete`.
6. Select an appropriate destination.
7. Click `Save`.

Remediate from Azure CLI

Use the below command to enable the Storage Logging for Blob service.

```
az storage logging update --account-name <storageAccountName> --account-key
<storageAccountKey> --services b --log rwd --retention 90
```

Default Value:

By default, storage account blob service logging is disabled for read, write, and delete operations.

References:

1. https://docs.microsoft.com/en-us/rest/api/storageservices/about-storage-analytics-logging
2. https://docs.microsoft.com/en-us/cli/azure/storage/logging?view=azure-cli-latest
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

Additional Information:

We cannot practically generalize detailed audit log requirements for every blob due to their nature and intent. This recommendation may be applicable to storage account blob service where security is paramount.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.14 Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests (Automated)

Profile Applicability:

- Level 2

Description:

Azure Table storage is a service that stores structured NoSQL data in the cloud, providing a key/attribute store with a schema-less design. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the tables. Storage Logging log entries contain the following information about individual requests: timing information such as start time, end-to-end latency, and server latency; authentication details; concurrency information; and the sizes of the request and response messages.

Rationale:

Storage Analytics logs contain detailed information about successful and failed requests to a storage service. This information can be used to monitor each individual request to a storage service for increased security or diagnostics. Requests are logged on a best-effort basis.

Storage Analytics logging is not enabled by default for your storage account.

Impact:

Being a level 2, enabling this setting can have a high impact on the cost of data storage used for logging more data per each request. Do not enable this without determining your need for this level of logging or forget to check in on data usage and projected cost.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Monitoring`, click `Diagnostics settings`.
3. Select the `table` tab indented below the storage account.
4. Ensure that at least one diagnostic setting is listed.
5. Click `Edit setting` on a diagnostic setting.
6. Ensure that at least one diagnostic setting has `StorageRead`, `StorageWrite`, and `StorageDelete` options selected under the `Logs` section and that they are sent to an appropriate destination.

Audit from Azure CLI

Ensure the below command's output contains properties delete, read and write set to true.

```
az storage logging show --services t --account-name <storageAccountName>
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL: https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 2fb86bf3-d221-43d1-96d1-2434af34eaa0 **- Name:** 'Configure diagnostic settings for Table Services to Log Analytics workspace'

Remediation:

Remediate from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Monitoring`, click `Diagnostics settings`.
3. Select the `table` tab indented below the storage account.
4. To create a new diagnostic setting, click `+ Add diagnostic setting`. To update an existing diagnostic setting, click `Edit setting` on the diagnostic setting.
5. Check the boxes next to `StorageRead`, `StorageWrite`, and `StorageDelete`.
6. Select an appropriate destination.
7. Click `Save`.

Remediate from Azure CLI

Use the below command to enable the Storage Logging for Table service.

```
az storage logging update --account-name <storageAccountName> --account-key
<storageAccountKey> --services t --log rwd --retention 90
```

Default Value:

By default, storage account table service logging is disabled for read, write, an delete operations

References:

1. https://docs.microsoft.com/en-us/rest/api/storageservices/about-storage-analytics-logging
2. https://docs.microsoft.com/en-us/cli/azure/storage/logging?view=azure-cli-latest
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

Additional Information:

We cannot practically generalize detailed audit log requirements for every table due to their nature and intent. This recommendation may be applicable to storage account table service where the security is paramount.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

4.15 Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2' (Automated)

Profile Applicability:

- Level 1

Description:

In some cases, Azure Storage sets the minimum TLS version to be version 1.0 by default. TLS 1.0 is a legacy version and has known vulnerabilities. This minimum TLS version can be configured to be later protocols such as TLS 1.2.

Rationale:

TLS 1.0 has known vulnerabilities and has been replaced by later versions of the TLS protocol. Continued use of this legacy protocol affects the security of data in transit.

Impact:

When set to TLS 1.2 all requests must leverage this version of the protocol. Applications leveraging legacy versions of the protocol will fail.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Settings`, click `Configuration`.
3. Ensure that the `Minimum TLS version` is set to `Version 1.2`.

Audit from Azure CLI

Get a list of all storage accounts and their resource groups

```
az storage account list | jq '.[] | {name, resourceGroup}'
```

Then query the minimumTLSVersion field

```
az storage account show \
    --name <storage-account> \
    --resource-group <resource-group> \
    --query minimumTlsVersion \
    --output tsv
```

Audit from PowerShell

To get the minimum TLS version, run the following command:

```
(Get-AzStorageAccount -Name <STORAGEACCOUNTNAME>  -ResourceGroupName
<RESOURCEGROUPNAME>).MinimumTlsVersion
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** fe83a0eb-a853-422d-aac2-1bffd182c5d0 **- Name:** 'Storage accounts should have the specified minimum TLS version'

Remediation:

Remediate from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Settings`, click `Configuration`.
3. Set the `Minimum TLS version` to `Version 1.2`.
4. Click `Save`.

Remediate from Azure CLI

```
az storage account update \
    --name <storage-account> \
    --resource-group <resource-group> \
    --min-tls-version TLS1_2
```

Remediate from PowerShell

To set the minimum TLS version, run the following command:

```
Set-AzStorageAccount -AccountName <STORAGEACCOUNTNAME> `
                     -ResourceGroupName <RESOURCEGROUPNAME> `
                     -MinimumTlsVersion TLS1_2
```

Default Value:

If a storage account is created through the portal, the MinimumTlsVersion property for that storage account will be set to TLS 1.2.

If a storage account is created through PowerShell or CLI, the MinimumTlsVersion property for that storage account will not be set, and defaults to TLS 1.0.

References:

1. https://docs.microsoft.com/en-us/azure/storage/common/transport-layer-security-configure-minimum-version?tabs=portal
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

4.16 Ensure 'Cross Tenant Replication' is not enabled (Automated)

Profile Applicability:

- Level 1

Description:

Cross Tenant Replication in Azure allows data to be replicated across multiple Azure tenants. While this feature can be beneficial for data sharing and availability, it also poses a significant security risk if not properly managed. Unauthorized data access, data leakage, and compliance violations are potential risks. Disabling Cross Tenant Replication ensures that data is not inadvertently replicated across different tenant boundaries without explicit authorization.

Rationale:

Disabling Cross Tenant Replication minimizes the risk of unauthorized data access and ensures that data governance policies are strictly adhered to. This control is especially critical for organizations with stringent data security and privacy requirements, as it prevents the accidental sharing of sensitive information.

Impact:

Disabling Cross Tenant Replication may affect data availability and sharing across different Azure tenants. Ensure that this change aligns with your organizational data sharing and availability requirements.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Data management`, click `Object replication`.
3. Click `Advanced settings`.
4. Ensure `Allow cross-tenant replication` is not checked.

Audit from Azure CLI

```
az storage account list --query "[*].[name,allowCrossTenantReplication]"
```

The value of `false` should be returned for each storage account listed.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 92a89a79-6c52-4a7e-a03f-61306fc49312 **- Name:** 'Storage accounts should prevent cross tenant object replication'

Remediation:

Remediate from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Data management`, click `Object replication`.
3. Click `Advanced settings`.
4. Uncheck `Allow cross-tenant replication`.
5. Click `OK`.

Remediate from Azure CLI

Replace the information within <> with appropriate values:

```
az storage account update --name <storageAccountName> --resource-group
<resourceGroupName> --allow-cross-tenant-replication false
```

Default Value:

For new storage accounts created after Dec 15, 2023 cross tenant replication is not enabled.

References:

1. https://learn.microsoft.com/en-us/azure/storage/blobs/object-replication-prevent-cross-tenant-policies?tabs=portal

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	13.4 Only Allow Access to Authorized Cloud Storage or Email Providers Only allow access to authorized cloud storage or email providers.		●	●

4.17 Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

The Azure Storage setting ‘Allow Blob Anonymous Access’ (aka "allowBlobPublicAccess") controls whether anonymous access is allowed for blob data in a storage account. When this property is set to True, it enables public read access to blob data, which can be convenient for sharing data but may carry security risks. When set to False, it disallows public access to blob data, providing a more secure storage environment.

Rationale:

If "Allow Blob Anonymous Access" is enabled, blobs can be accessed by adding the blob name to the URL to see the contents. An attacker can enumerate a blob using methods, such as brute force, and access them.

Exfiltration of data by brute force enumeration of items from a storage account may occur if this setting is set to 'Enabled'.

Impact:

Additional consideration may be required for exceptional circumstances where elements of a storage account require public accessibility. In these circumstances, it is highly recommended that all data stored in the public facing storage account be reviewed for sensitive or potentially compromising data, and that sensitive or compromising data is never stored in these storage accounts.

Audit:

Audit from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Settings`, click `Configuration`.
3. Ensure `Allow Blob Anonymous Access` is set to `Disabled`.

Audit from Azure CLI

For every storage account in scope:

```
az storage account show --name "<yourStorageAccountName>" --query
allowBlobPublicAccess
```

Ensure that every storage account in scope returns `false` for the "allowBlobPublicAccess" setting.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 4fa4b6c0-31ca-4c0d-b10d-24b96f62a751 **- Name:** '[Preview]: Storage account public access should be disallowed'

Remediation:

Remediate from Azure Portal

1. Go to `Storage Accounts`.
2. For each storage account, under `Settings`, click `Configuration`.
3. Set `Allow Blob Anonymous Access` to `Disabled`.
4. Click `Save`.

Remediate from Powershell

For every storage account in scope, run the following:

```
$storageAccount = Get-AzStorageAccount -ResourceGroupName
"<yourResourceGroup>" -Name "<yourStorageAccountName>"
$storageAccount.AllowBlobPublicAccess = $false
Set-AzStorageAccount -InputObject $storageAccount
```

Default Value:

Disabled

References:

1. https://learn.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent?tabs=portal
2. https://learn.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent?source=recommendations&tabs=portal
3. Classic Storage Accounts: https://learn.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent-classic?tabs=portal

Additional Information:

Azure Storage accounts that use the classic deployment model will be retired on August 31, 2024.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

5 Database Services

This section covers security recommendations to follow to set general database services policies on an Azure Subscription. Subsections will address specific database types.

5.1 Azure SQL Database

This section covers security best practice recommendations for Azure SQL Database.

Azure Product Page: https://azure.microsoft.com/en-us/products/azure-sql/database/

5.1.1 Ensure that 'Auditing' is set to 'On' (Automated)

Profile Applicability:

- Level 1

Description:

Enable auditing on SQL Servers.

Rationale:

The Azure platform allows a SQL server to be created as a service. Enabling auditing at the server level ensures that all existing and newly created databases on the SQL server instance are audited. Auditing policy applied on the SQL database does not override auditing policy and settings applied on the particular SQL server where the database is hosted.

Auditing tracks database events and writes them to an audit log in the Azure storage account. It also helps to maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.

Audit:

Audit from Azure Portal

1. Go to `SQL servers`
2. For each server instance
3. Under `Security`, click `Auditing`
4. Ensure that `Enable Azure SQL Auditing` is set to `On`

Audit from PowerShell

Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server

```
Get-AzSqlServerAudit -ResourceGroupName <ResourceGroupName> -ServerName
<SQLServerName>
```

Ensure that `BlobStorageTargetState`, `EventHubTargetState`, or `LogAnalyticsTargetState` is set to `Enabled`.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** [a6fb4358-5bf4-4ad7-ba82-2cd2f41ce5e9](a6fb4358-5bf4-4ad7-ba82-2cd2f41ce5e9) **- Name:** 'Auditing on SQL server should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `SQL servers`
2. Select the SQL server instance
3. Under `Security`, click `Auditing`
4. Click the toggle next to `Enable Azure SQL Auditing`
5. Select an Audit log destination
6. Click `Save`

Remediate from PowerShell

Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server, enable auditing and set the retention for at least 90 days.

Log Analytics Example

```
Set-AzSqlServerAudit -ResourceGroupName <resource group name> -ServerName
<SQL Server name> -RetentionInDays <Number of Days to retain the audit logs,
should be 90days minimum> -LogAnalyticsTargetState Enabled -
WorkspaceResourceId "/subscriptions/<subscription
ID>/resourceGroups/insights-
integration/providers/Microsoft.OperationalInsights/workspaces/<workspace
name>
```

Event Hub Example

```
Set-AzSqlServerAudit -ResourceGroupName "<resource group name>" -ServerName
"<SQL Server name>" -EventHubTargetState Enabled -EventHubName
    "<Event Hub name>" -EventHubAuthorizationRuleResourceId "<Event Hub
Authorization Rule Resource ID>"
```

Blob Storage Example

```
Set-AzSqlServerAudit -ResourceGroupName "<resource group name>" -ServerName
"<SQL Server name>" -BlobStorageTargetState Enabled
    -StorageAccountResourceId
"/subscriptions/<subscription_ID>/resourceGroups/<Resource_Group>/providers/M
icrosoft.Stora
    ge/storageAccounts/<Storage Account name>"
```

Default Value:

By default, `Enable Azure SQL Auditing` is set to `Off`.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-auditing-on-sql-servers

2. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermsqlserverauditing?view=azurermps-5.2.0
3. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserverauditingpolicy?view=azurermps-5.2.0
4. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

Additional Information:

- A server policy applies to all existing and newly created databases on the server.
- If server blob auditing is enabled, it always applies to the database. The database will be audited, regardless of the database auditing settings. Auditing type table is already deprecated leaving only type blob available.
- Enabling blob auditing on the database, in addition to enabling it on the server, does not override or change any of the settings of the server blob auditing. Both audits will exist side by side. In other words, the database is audited twice in parallel; once by the server policy and once by the database policy.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

5.1.2 Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that no SQL Databases allow ingress from 0.0.0.0/0 (ANY IP).

Rationale:

Azure SQL Server includes a firewall to block access to unauthorized connections. More granular IP addresses can be defined by referencing the range of addresses available from specific datacenters.

By default, for a SQL server, a Firewall exists with StartIp of 0.0.0.0 and EndIP of 0.0.0.0 allowing access to all the Azure services.

Additionally, a custom rule can be set up with StartIp of 0.0.0.0 and EndIP of 255.255.255.255 allowing access from ANY IP over the Internet.

In order to reduce the potential attack surface for a SQL server, firewall rules should be defined with more granular IP addresses by referencing the range of addresses available from specific datacenters.

If `Allow Azure services and resources to access this server` is 'Checked', this will allow resources outside of the subscription/tenant/organization boundary, within any region of Azure, to effectively bypass the defined SQL Server Network ACL on public endpoint. A malicious attacker can successfully launch a SQL server password bruteforce attack by creating a virtual machine in any Azure subscription/region, from outside of the subscription boundary where the SQL Server is residing.

Impact:

Disabling `Allow Azure services and resources to access this server` will break all connections to SQL server and Hosted Databases unless custom IP specific rules are added in Firewall Policy.

Audit:

Audit from Azure Portal

1. Go to `SQL servers`
2. For each SQL server
3. Under `Security`, click `Networking`
4. Ensure that `Allow Azure services and resources to access this server` is unchecked
5. Ensure that no firewall rule exists with

- Start IP of `0.0.0.0`
- or other combinations which allows access to wider public IP ranges

Audit from Azure CLI
List all SQL servers

```
az sql server list
```

For each SQL server run the following command

```
az sql server firewall-rule list --resource-group <resource group name> --
server <sql server name>
```

Ensure the output does not contain any firewall `allow` rules with a source of `0.0.0.0`, or any rules named `AllowAllWindowsAzureIps`

Audit from PowerShell
Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server

```
Get-AzSqlServerFirewallRule -ResourceGroupName <resource group name> -
ServerName <server name>
```

Ensure that `StartIpAddress` is not set to `0.0.0.0`, `/0` or other combinations which allows access to wider public IP ranges including Windows Azure IP ranges. Also ensure that `FirewallRuleName` doesn't contain `AllowAllWindowsAzureIps` which is the rule created when the `Allow Azure services and resources to access this server` setting is enabled for that SQL Server.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 1b8ca024-1d5c-4dec-8995-b1a932b41780 **- Name:** 'Public network access on Azure SQL Database should be disabled'

Remediation:

Remediate from Azure Portal

1. Go to `SQL servers`
2. For each SQL server
3. Under `Security`, click `Networking`
4. Uncheck `Allow Azure services and resources to access this server`

5. Set firewall rules to limit access to only authorized connections
6. Click Save

Remediate from Azure CLI

Disable default firewall rule Allow access to Azure services:

```
az sql server firewall-rule delete --resource-group <resource group> --server
<sql server name> --name "AllowAllWindowsAzureIps"
```

Remove a custom firewall rule:

```
az sql server firewall-rule delete --resource-group <resource group> --server
<sql server name> --name <firewall rule name>
```

Create a firewall rule:

```
az sql server firewall-rule create --resource-group <resource group> --server
<sql server name> --name <firewall rule name> --start-ip-address "<IP Address
other than 0.0.0.0>" --end-ip-address "<IP Address other than 0.0.0.0 or
255.255.255.255>"
```

Update a firewall rule:

```
az sql server firewall-rule update --resource-group <resource group> --server
<sql server name> --name <firewall rule name> --start-ip-address "<IP Address
other than 0.0.0.0>" --end-ip-address "<IP Address other than 0.0.0.0 or
255.255.255.255>"
```

Remediate from PowerShell

Disable Default Firewall Rule Allow access to Azure services :

```
Remove-AzSqlServerFirewallRule -FirewallRuleName "AllowAllWindowsAzureIps" -
ResourceGroupName <resource group name> -ServerName <server name>
```

Remove a custom Firewall rule:

```
Remove-AzSqlServerFirewallRule -FirewallRuleName "<firewall rule name>" -
ResourceGroupName <resource group name> -ServerName <server name>
```

Set the appropriate firewall rules:

```
Set-AzSqlServerFirewallRule -ResourceGroupName <resource group name> -
ServerName <server name> -FirewallRuleName "<firewall rule name>" -
StartIpAddress "<IP Address other than 0.0.0.0>" -EndIpAddress "<IP Address
other than 0.0.0.0 or 255.255.255.255>"
```

Default Value:

By default, Allow access to Azure Services is set to NO.

References:

1. https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-windows-firewall-for-database-engine-access?view=sql-server-2017

2. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermsqlserverfirewallrule?view=azurermps-5.2.0
3. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserverfirewallrule?view=azurermps-5.2.0
4. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/remove-azurermsqlserverfirewallrule?view=azurermps-5.2.0
5. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-firewall-configure
6. https://docs.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/sp-set-database-firewall-rule-azure-sql-database?view=azuresqldb-current
7. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls
8. https://learn.microsoft.com/en-us/azure/azure-sql/database/network-access-controls-overview?view=azuresql#allow-azure-services

Additional Information:

Firewall rules configured on individual SQL Database using Transact-sql overrides the rules set on SQL server. Azure does not provide any Powershell, API, CLI, Portal option to check database level firewall rules, and so far Transact-SQL is the only way to check for the same. For comprehensive control over egress traffic on SQL Databases, Firewall rules should be checked using SQL client.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

5.1.3 Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key (Automated)

Profile Applicability:

- Level 2

Description:

Transparent Data Encryption (TDE) with Customer-managed key support provides increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties.

With TDE, data is encrypted at rest with a symmetric key (called the database encryption key) stored in the database or data warehouse distribution. To protect this data encryption key (DEK) in the past, only a certificate that the Azure SQL Service managed could be used. Now, with Customer-managed key support for TDE, the DEK can be protected with an asymmetric key that is stored in the Azure Key Vault. The Azure Key Vault is a highly available and scalable cloud-based key store which offers central key management, leverages FIPS 140-2 Level 2 validated hardware security modules (HSMs), and allows separation of management of keys and data for additional security.

Based on business needs or criticality of data/databases hosted on a SQL server, it is recommended that the TDE protector is encrypted by a key that is managed by the data owner (Customer-managed key).

Rationale:

Customer-managed key support for Transparent Data Encryption (TDE) allows user control of TDE encryption keys and restricts who can access them and when. Azure Key Vault, Azure's cloud-based external key management system, is the first key management service where TDE has integrated support for Customer-managed keys. With Customer-managed key support, the database encryption key is protected by an asymmetric key stored in the Key Vault. The asymmetric key is set at the server level and inherited by all databases under that server.

Impact:

Once TDE protector is encrypted with a Customer-managed key, it transfers entire responsibility of respective key management on to you, and hence you should be more careful about doing any operations on the particular key in order to keep data from corresponding SQL server and Databases hosted accessible.

When deploying Customer Managed Keys, it is prudent to ensure that you also deploy an automated toolset for managing these keys (this should include discovery and key rotation), and Keys should be stored in an HSM or hardware backed keystore, such as Azure Key Vault.

As far as toolsets go, check with your cryptographic key provider, as they may well provide one as an add-on to their service.

Audit:

Audit from Azure Portal

1. Go to `SQL servers`
2. For each SQL server, under `Security`, click `Transparent data encryption`
3. Ensure that `Customer-managed key` is selected
4. Ensure `Make this key the default TDE protector` is checked

Audit from Azure CLI

```
az account get-access-token --query
"{subscripton:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/resourceGroups/{resourceGroupNa
me}/providers/Microsoft.Sql/servers/{serverName}/encryptionProtector?api-
version=2015-05-01-preview'
```

Ensure the output of the command contains properties
`kind` set to `azurekeyvault`
`serverKeyType` set to `AzureKeyVault`
`uri` is not null

Audit from PowerShell

```
Get-AzSqlServerTransparentDataEncryptionProtector -ServerName <ServerName> -
ResourceGroupName <ResourceGroupName>
```

Ensure the output of the command contains properties
`Type` set to `AzureKeyVault`
`ServerKeyVaultKeyName` set to `KeyVaultName_KeyName_KeyIdentifierVersion`
`KeyId` set to `KeyIdentifier`

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 0a370ff3-6cab-4e85-8995-295fd854c5b8 **- Name:** 'SQL servers should use customer-managed keys to encrypt data at rest'
- **Policy ID:** ac01ad65-10e5-46df-bdd9-6b0cad13e1d2 **- Name:** 'SQL managed instances should use customer-managed keys to encrypt data at rest'

Remediation:

Remediate from Azure Portal

1. Go to `SQL servers`
2. For each SQL server, under `Security`, click `Transparent data encryption`
3. Set `Transparent data encryption` to `Customer-managed key`
4. Select a key or enter a key identifier
5. Check `Make this key the default TDE protector`
6. Click `Save`

Remediate from Azure CLI

Use the below command to encrypt SQL server's TDE protector with a Customer-managed key

```
az sql server tde-key set --resource-group <resourceName> --server
<dbServerName> --server-key-type {AzureKeyVault} --kid <keyIdentifier>
```

Remediate from PowerShell

Use the below command to encrypt SQL server's TDE protector with a Customer-managed Key Vault key

```
Set-AzSqlServerTransparentDataEncryptionProtector -Type AzureKeyVault -KeyId
<KeyIdentifier> -ServerName <ServerName> -ResourceGroupName
<ResourceGroupName>
```

Select `Y` when prompted

Default Value:

By Default, Microsoft managed TDE protector is enabled for a SQL server.

References:

1. https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption-byok-azure-sql
2. https://azure.microsoft.com/en-in/blog/preview-sql-transparent-data-encryption-tde-with-bring-your-own-key-support/
3. https://winterdom.com/2017/09/07/azure-sql-tde-protector-keyvault
4. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required
5. https://docs.microsoft.com/en-us/azure/key-vault/general/basic-concepts
6. https://docs.microsoft.com/en-us/cli/azure/sql/server/tde-key?view=azure-cli-latest
7. https://learn.microsoft.com/en-us/powershell/module/az.sql/get-azsqlservertransparentdataencryptionprotector?view=azps-9.2.0
8. https://learn.microsoft.com/en-us/powershell/module/az.sql/set-azsqlservertransparentdataencryptionprotector?view=azps-9.2.0

Additional Information:

- This configuration is audited or can be done only on SQL server. The same configuration will be in effect on SQL Databases hosted on SQL Server.
- Ensuring TDE is protected by a Customer-managed key on SQL Server does not ensure the encryption of SQL Databases. `Transparent Data Encryption : Data Encryption (ON/OFF)` setting on individual SQL Database decides whether database is encrypted or not.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	16.4 Encrypt or Hash all Authentication Credentials Encrypt or hash with a salt all authentication credentials when stored.		●	●

5.1.4 Ensure that Microsoft Entra authentication is Configured for SQL Servers (Automated)

Profile Applicability:

- Level 1

Description:

Use Microsoft Entra authentication for authentication with SQL Database to manage credentials in a single place.

Rationale:

Microsoft Entra authentication is a mechanism to connect to Microsoft Azure SQL Database and SQL Data Warehouse by using identities in the Microsoft Entra ID directory. With Entra ID authentication, identities of database users and other Microsoft services can be managed in one central location. Central ID management provides a single place to manage database users and simplifies permission management.

- It provides an alternative to SQL Server authentication.
- Helps stop the proliferation of user identities across database servers.
- Allows password rotation in a single place.
- Customers can manage database permissions using external (Entra ID) groups.
- It can eliminate storing passwords by enabling integrated Windows authentication and other forms of authentication supported by Microsoft Entra.
- Entra ID authentication uses contained database users to authenticate identities at the database level.
- Entra ID supports token-based authentication for applications connecting to SQL Database.
- Entra ID authentication supports ADFS (domain federation) or native user/password authentication for a local Active Directory without domain synchronization.
- Entra ID supports connections from SQL Server Management Studio that use Active Directory Universal Authentication, which includes Multi-Factor Authentication (MFA). MFA includes strong authentication with a range of easy verification options — phone call, text message, smart cards with pin, or mobile app notification.

Impact:

This will create administrative overhead with user account and permission management. For further security on these administrative accounts, you may want to consider licensing which supports features like Multi Factor Authentication.

Audit:

Audit from Azure Portal

1. Go to `SQL servers`
2. For each SQL server, under `Settings`, click `Microsoft Entra ID`
3. Under `Microsoft Entra admin`, ensure a value has been set for `Admin Name`

Audit from Azure CLI

To list SQL Server Admins on a specific server:

```
az sql server ad-admin list --resource-group <resource-group> --server
<server>
```

Audit from PowerShell

Print a list of all SQL Servers to find which one you want to audit

```
Get-AzSqlServer
```

Audit a list of Administrators on a Specific Server

```
Get-AzSqlServerActiveDirectoryAdministrator -ResourceGroupName <resource
group name> -ServerName <server name>
```

Ensure Output shows `DisplayName` set to `AD account`.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 1f314764-cb73-4fc9-b863-8eca98ac36e9 **- Name:** 'An Azure Active Directory administrator should be provisioned for SQL servers'

Remediation:

Remediate from Azure Portal

1. Go to `SQL servers`
2. For each SQL server, under `Settings`, click `Microsoft Entra ID`
3. Click `Set admin`
4. Select an admin
5. Click `Select`
6. Click `Save`

Remediate from Azure CLI

```
az ad user show --id
```

For each Server, set AD Admin

```
az sql server ad-admin create --resource-group <resource group name> --server
<server name> --display-name <display name> --object-id <object id of user>
```

Remediate from PowerShell
For each Server, set Entra ID Admin

```
Set-AzSqlServerActiveDirectoryAdministrator -ResourceGroupName <resource
group name> -ServerName <server name> -DisplayName "<Display name of AD
account to set as DB administrator>"
```

Default Value:

Entra ID Authentication for SQL Database/Server is not enabled by default

References:

1. https://learn.microsoft.com/en-us/azure/azure-sql/database/authentication-aad-configure
2. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication
3. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermsqlserveractivedirectoryadministrator?view=azurermps-5.2.0
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-1-use-centralized-identity-and-authentication-system
5. https://docs.microsoft.com/en-us/cli/azure/sql/server/ad-admin?view=azure-cli-latest#az_sql_server_ad_admin_list

Additional Information:

NOTE - Assigning an Administrator in Entra ID is just the first step. When using Entra ID for central authentication there are many other groups and roles that need to be configured base on the needs of your organization. The How-to Guides should be used to determine what roles should be assigned and what groups should be created to manage permissions and access to resources.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

5.1.5 Ensure that 'Data encryption' is set to 'On' on a SQL Database (Automated)

Profile Applicability:

- Level 1

Description:

Enable Transparent Data Encryption on every SQL server.

Rationale:

Azure SQL Database transparent data encryption helps protect against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

Audit:

Audit from Azure Portal

1. Go to `SQL databases`
2. For each DB instance, under `Security`, click `Data Encryption`
3. Under `Transparent data encryption`, ensure that `Data encryption` is set to `On`

Audit from Azure CLI

Ensure the output of the below command is `Enabled`

```
az sql db tde show --resource-group <resourceGroup> --server <dbServerName> -
-database <dbName> --query status
```

Audit from PowerShell

Get a list of SQL Servers.

```
Get-AzSqlServer
```

For each server, list the databases.

```
Get-AzSqlDatabase -ServerName <SQL Server Name> -ResourceGroupName <Resource
Group Name>
```

For each database not listed as a `Master` database, check for Transparent Data Encryption.

```
Get-AzSqlDatabaseTransparentDataEncryption -ResourceGroupName <Resource Group
Name> -ServerName <SQL Server Name> -DatabaseName <Database Name>
```

Make sure `DataEncryption` is `Enabled` for each database except the `Master` database.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 17k78e20-9358-41c9-923c-fb736d382a12 **- Name:** 'Transparent Data Encryption on SQL databases should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `SQL databases`
2. For each DB instance, under `Security`, click `Data Encryption`
3. Under `Transparent data encryption`, set `Data encryption` to `On`
4. Click `Save`

Remediate from Azure CLI
Use the below command to enable `Transparent data encryption` for SQL DB instance.

```
az sql db tde set --resource-group <resourceGroup> --server <dbServerName> --
database <dbName> --status Enabled
```

Remediate from PowerShell
Use the below command to enable `Transparent data encryption` for SQL DB instance.

```
Set-AzSqlDatabaseTransparentDataEncryption -ResourceGroupName <Resource Group
Name> -ServerName <SQL Server Name> -DatabaseName <Database Name> -State
'Enabled'
```

Note:

- TDE cannot be used to encrypt the logical master database in SQL Database. The master database contains objects that are needed to perform the TDE operations on the user databases.
- Azure Portal does not show master databases per SQL server. However, CLI/API responses will show master databases.

Default Value:

By default, `Data encryption` is set to `On`.

References:

1. https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption-with-azure-sql-database

2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-4-enable-data-at-rest-encryption-by-default
3. https://learn.microsoft.com/en-us/powershell/module/az.sql/set-azsqldatabasetransparentdataencryption?view=azps-9.2.0

Additional Information:

- Transparent Data Encryption (TDE) can be enabled or disabled on individual `SQL Database` level and not on the `SQL Server` level.
- TDE cannot be used to encrypt the logical master database in SQL Database. The master database contains objects that are needed to perform the TDE operations on the user databases.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

5.1.6 Ensure that 'Auditing' Retention is 'greater than 90 days' (Automated)

Profile Applicability:

- Level 1

Description:

SQL Server Audit Retention should be configured to be greater than 90 days.

Rationale:

Audit Logs can be used to check for anomalies and give insight into suspected breaches or misuse of information and access.

Audit:

Audit from Azure Portal

1. Go to `SQL servers`.
2. For each SQL server, under `Security`, click `Auditing`.
3. If `Storage` is checked, expand `Advanced properties`.
4. Ensure `Retention (days)` is set to a value greater than `90`, or `0` for unlimited retention.

Audit from PowerShell

Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server

```
Get-AzSqlServerAudit -ResourceGroupName <resource group name> -ServerName
<server name>
```

Ensure that `RetentionInDays` is set to `more than 90`

Note: If the SQL server is set with `LogAnalyticsTargetState` setting set to `Enabled`, run the following additional command.

```
Get-AzOperationalInsightsWorkspace | Where-Object {$_.ResourceId -eq <SQL
Server WorkSpaceResourceId>}
```

Ensure that `RetentionInDays` is set to `more than 90`

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 89099bee-89e0-4b26-a5f4-165451757743 **- Name:** 'SQL servers with auditing to storage account destination should be configured with 90 days retention or higher'

Remediation:

Remediate from Azure Portal

1. Go to `SQL servers`.
2. For each SQL server, under `Security`, click `Auditing`.
3. If `Storage` is checked, expand `Advanced properties`.
4. Set `Retention (days)` to a value greater than `90`, or `0` for unlimited retention.
5. Click `Save`.

Remediate from PowerShell
For each Server, set retention policy to more than 90 days
Log Analytics Example

```
Set-AzSqlServerAudit -ResourceGroupName <resource group name> -ServerName
<SQL Server name> -RetentionInDays <Number of Days to retain the audit logs,
should be more than 90 days> -LogAnalyticsTargetState Enabled -
WorkspaceResourceId "/subscriptions/<subscription
ID>/resourceGroups/insights-
integration/providers/Microsoft.OperationalInsights/workspaces/<workspace
name>
```

Event Hub Example

```
Set-AzSqlServerAudit -ResourceGroupName "<resource group name>" -ServerName
"<SQL Server name>" -EventHubTargetState Enabled -EventHubName
    "<Event Hub name>" -EventHubAuthorizationRuleResourceId "<Event Hub
Authorization Rule Resource ID>"
```

Blob Storage Example

```
Set-AzSqlServerAudit -ResourceGroupName "<resource group name>" -ServerName
"<SQL Server name>" -BlobStorageTargetState Enabled
    -StorageAccountResourceId
"/subscriptions/<subscription_ID>/resourceGroups/<Resource_Group>/providers/M
icrosoft.Stora
    ge/storageAccounts/<Storage Account name>"
```

Default Value:

By default, SQL Server audit storage is `disabled`.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing
2. https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermsqlserverauditing?view=azurermps-5.2.0
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-6-configure-log-storage-retention

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise’s audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

5.1.7 Ensure Public Network Access is Disabled (Manual)

Profile Applicability:

- Level 1

Description:

Disabling public network access restricts the service from accessing public networks.

Rationale:

A secure network architecture requires carefully constructed network segmentation. Public Network Access tends to be overly permissive and introduces unintended vectors for threat activity.

Impact:

Some architectural consideration may be necessary to ensure that required network connectivity is still made available. No additional cost or performance impact is required to deploy this recommendation.

Audit:

From Azure Portal

1. Go to `SQL servers`.
2. For each SQL server, under `Security`, click `Networking`.
3. Ensure that `Public network access` is set to `Disable`.

Remediation:

From Azure Portal

1. Go to `SQL servers`.
2. For each SQL server, under `Security`, click `Networking`.
3. Set `Public network access` to `Disable`.
4. Click `Save`.

Default Value:

By default, Azure SQL Server's Public network access is set to `Disable`.

References:

1. https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-2-secure-cloud-services-with-network-controls
2. https://learn.microsoft.com/en-us/azure/azure-sql/database/connectivity-settings?view=azuresql&tabs=azure-portal#deny-public-network-access

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

5.2 Azure Database for PostgreSQL

This section covers security best practice recommendations for Azure PostgreSQL Database Servers.

Azure Product Page: https://azure.microsoft.com/en-us/products/postgresql/

RETIREMENT of Azure PostgreSQL Single Server: Azure PostgreSQL Single Server is slated for retirement by March 25, 2025. Azure PostgreSQL Flexible Server is the newer deployment standard and is unaffected. Please use these resources to consider and prepare for migration:

- https://learn.microsoft.com/en-us/azure/postgresql/single-server/whats-happening-to-postgresql-single-server
- https://learn.microsoft.com/en-us/azure/postgresql/migrate/concepts-single-to-flexible

5.2.1 Ensure server parameter 'require_secure_transport' is set to 'ON' for PostgreSQL flexible server (Automated)

Profile Applicability:

- Level 1

Description:

Enable `require_secure_transport` on `PostgreSQL flexible servers`.

Rationale:

`SSL connectivity` helps to provide a new layer of security by connecting database server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between database server and client applications helps protect against "man in the middle" attacks by encrypting the data stream between the server and application.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for PostgreSQL flexible servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `require_secure_transport`.
5. Ensure that the `VALUE` for `require_secure_transport` is set to `ON`.

Audit from Azure CLI
Ensure the below command returns a `value` of `on`:

```
az postgres flexible-server parameter show --resource-group <resourceGroup> --server-name <serverName> --name require_secure_transport
```

Audit from PowerShell
Ensure the below command returns a `Value` of `on`:

```
Get-AzPostgreSqlFlexibleServerConfiguration -ResourceGroupName
<resourceGroup> -ServerName <serverName> -Name require_secure_transport
```

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** c29c38cb-74a7-4505-9a06-e588ab86620a **- Name:** 'Enforce SSL connection should be enabled for PostgreSQL flexible servers'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for PostgreSQL flexible servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `require_secure_transport`.
5. Set the `VALUE` for `require_secure_transport` to `ON`.
6. Click `Save`.

Remediate from Azure CLI

Use the below command to enable `require_secure_transport`:

```
az postgres flexible-server parameter set --resource-group <resourceGroup> --
server-name <serverName> --name require_secure_transport --value on
```

Remediate from PowerShell

```
Update-AzPostgreSqlFlexibleServerConfiguration -ResourceGroupName
<resourceGroup> -ServerName <serverName> -Name require_secure_transport -
Value on
```

Default Value:

By default, secure connectivity is enforced, but some application frameworks may not enable it during deployment.

References:

1. https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/concepts-networking-ssl-tls
2. https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/how-to-connect-tls-ssl
3. https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlflexibleserverconfiguration?view=azps-12.2.0#example-1-get-specified-postgresql-configuration-by-name
4. https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlflexibleserverconfiguration?view=azps-12.2.0#example-1-updatae-specified-postgresql-configuration-by-name
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

5.2.2 Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL flexible server (Automated)

Profile Applicability:

- Level 1

Description:

Enable `log_checkpoints` on `PostgreSQL flexible servers`.

Rationale:

Enabling `log_checkpoints` helps the PostgreSQL Database to `Log each checkpoint`, which in turn generates query and error logs. However, access to transaction logs is not supported. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Go to `Azure Database for PostgreSQL flexible servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `log_checkpoints`.
5. Ensure that the `VALUE` for `log_checkpoints` is set to `ON`.

Audit from Azure CLI

Ensure the below command returns a `value` of `on`:

```
az postgres flexible-server parameter show --resource-group <resourceGroup> -
-server-name <serverName> --name log_checkpoints
```

Audit from PowerShell

Ensure the below command returns a `Value` of `on`:

```
Get-AzPostgreSqlFlexibleServerConfiguration -ResourceGroupName
<resourceGroup> -ServerName <serverName> -Name log_checkpoints
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 70be9e12-c935-49ac-9bd8-fd64b85c1f87 **- Name:** 'Log checkpoints should be enabled for PostgreSQL flexible servers'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Go to `Azure Database for PostgreSQL flexible servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `log_checkpoints`.
5. Set the `VALUE` for `log_checkpoints` to `ON`.
6. Click `Save`.

Remediate from Azure CLI
Use the below command to enable `log_checkpoints`:

```
az postgres flexible-server parameter set --resource-group <resourceGroup> --
server-name <serverName> --name log_checkpoints --value on
```

Remediate from PowerShell

```
Update-AzPostgreSqlFlexibleServerConfiguration -ResourceGroupName
<resourceGroup> -ServerName <serverName> -Name log_checkpoints -Value on
```

Default Value:

By default `log_checkpoints` is enabled (set to `on`).

References:

1. https://learn.microsoft.com/en-us/rest/api/postgresql/flexibleserver/configurations/list-by-server
2. https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/how-to-configure-server-parameters-using-portal
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
4. https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/concepts-logging#configure-logging
5. https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlflexibleserverconfiguration?view=azps-12.2.0#example-1-get-specified-postgresql-configuration-by-name
6. https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlflexibleserverconfiguration?view=azps-12.2.0#example-1-updatae-specified-postgresql-configuration-by-name

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise’s audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.2.3 Ensure server parameter 'connection_throttle.enable' is set to 'ON' for PostgreSQL flexible server (Automated)

Profile Applicability:

- Level 1

Description:

Enable connection throttling on `PostgreSQL flexible servers`.

Rationale:

Enabling `connection throttling` helps the PostgreSQL Database to `Set the verbosity of logged messages`. This in turn generates query and error logs with respect to concurrent connections that could lead to a successful Denial of Service (DoS) attack by exhausting connection resources. A system can also fail or be degraded by an overload of legitimate users. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for PostgreSQL flexible servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `connection_throttle.enable`.
5. Ensure that `VALUE` for `connection_throttle.enable` is set to `ON`.

Audit from Azure CLI

Ensure the below command returns a `value` of `on`:

```
az postgres flexible-server parameter show --resource-group <resourceGroup> -
-server-name <serverName> --name connection_throttle.enable
```

Audit from PowerShell

Ensure the below command returns a `Value` of `on`:

```
Get-AzPostgreSqlFlexibleServerConfiguration -ResourceGroupName
<resourceGroup> -ServerName <serverName> -Name connection_throttle.enable
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** dacf07fa-0eea-4486-80bc-b93fae88ac40 **- Name:** 'Connection throttling should be enabled for PostgreSQL flexible servers'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for PostgreSQL flexible servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `connection_throttle.enable`.
5. Set `connection_throttle.enable` to `ON`.
6. Click `Save`.

Remediate from Azure CLI

Use the below command to enable `connection_throttle.enable`:

```
az postgres flexible-server parameter set --resource-group <resourceGroup> --
server-name <serverName> --name connection_throttle.enable --value on
```

Remediate from PowerShell

Use the below command to update `connection_throttling` configuration.

```
Update-AzPostgreSqlFlexibleServerConfiguration -ResourceGroupName
<resourceGroup> -ServerName <serverName> -Name connection_throttle.enable -
Value on
```

Default Value:

By default, `connection_throttle.enable` is disabled (set to `off`).

References:

1. https://learn.microsoft.com/en-us/rest/api/postgresql/flexibleserver/configurations/list-by-server
2. https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/how-to-configure-server-parameters-using-portal
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
4. https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlflexibleserverconfiguration?view=azps-12.2.0#example-1-get-specified-postgresql-configuration-by-name
5. https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlflexibleserverconfiguration?view=azps-12.2.0#example-1-updatae-specified-postgresql-configuration-by-name

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise’s audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.2.4 Ensure server parameter 'logfiles.retention_days' is greater than 3 days for PostgreSQL flexible server (Automated)

Profile Applicability:

- Level 1

Description:

Ensure `logfiles.retention_days` on `PostgreSQL flexible servers` is set to an appropriate value.

Rationale:

Configuring `logfiles.retention_days` determines the duration in days that `Azure Database for PostgreSQL` retains log files. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

Impact:

Configuring this setting will result in logs being retained for the specified number of days. If this is configured on a high traffic server, the log may grow quickly to occupy a large amount of disk space. In this case you may want to set this to a lower number.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Go to `Azure Database for PostgreSQL flexible servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `logfiles.retention_days`.
5. Ensure that the `VALUE` is between 4 and 7 (inclusive).

Audit from Azure CLI
Ensure `logfiles.retention_days` value is greater than 3.

```
az postgres flexible-server parameter show --resource-group <resourceGroup> --server-name <serverName> --name logfiles.retention_days
```

Audit from Powershell
Ensure `logfiles.retention_days` value is greater than 3:

```
Get-AzPostgreSqlFlexibleServerConfiguration -ResourceGroupName <resourceGroup> -ServerName <serverName> -Name logfiles.retention_days
```

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Go to `Azure Database for PostgreSQL flexible servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `logfiles.retention_days`.
5. Input a value between 4 and 7 (inclusive).
6. Click `Save`.

Remediate from Azure CLI

Use the below command to update `logfiles.retention_days` configuration:

```
az postgres flexible-server parameter set --resource-group <resourceGroup> --
server-name <serverName> --name logfiles.retention_days --value <4-7>
```

Remediate from Powershell

Use the below command to update `logfiles.retention_days` configuration:

```
Update-AzPostgreSqlFlexibleServerConfiguration -ResourceGroupName
<resourceGroup> -ServerName <serverName> -Name logfiles.retention_days -Value
<4-7>
```

Default Value:

By default `logfiles.retention_days` is set to `3`.

References:

1. https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/how-to-configure-server-parameters-using-portal
2. https://learn.microsoft.com/en-us/rest/api/postgresql/flexibleserver/configurations/list-by-server
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-6-configure-log-storage-retention
4. https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlflexibleserverconfiguration?view=azps-12.2.0#example-1-get-specified-postgresql-configuration-by-name
5. https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlflexibleserverconfiguration?view=azps-12.2.0#example-1-updatae-specified-postgresql-configuration-by-name

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise’s audit log management process.	●	●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

5.2.5 Ensure 'Allow public access from any Azure service within Azure to this server' for PostgreSQL flexible server is disabled (Automated)

Profile Applicability:

- Level 1

Description:

Disable access from Azure services to `PostgreSQL flexible server`.

Rationale:

If access from Azure services is enabled, the server's firewall will accept connections from all Azure resources, including resources not in your subscription. This is usually not a desired configuration. Instead, set up firewall rules to allow access from specific network ranges or VNET rules to allow access from specific virtual networks.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for PostgreSQL flexible servers`.
3. For each database, under `Settings`, click `Networking`.
4. Under `Firewall rules`, ensure `Allow public access from any Azure service within Azure to this server` is not checked.

Audit from Azure CLI

Ensure the below command does not return a rule with a name beginning `AllowAllAzureServicesAndResourcesWithinAzureIps` **or** with `"startIpAddress": "0.0.0.0"` **or** `"endIpAddress": "0.0.0.0"`:

```
az postgres flexible-server firewall-rule list --resource-group
<resourceGroup> --name <serverName>
```

Audit from PowerShell

Ensure the below command does not return a rule with a name beginning `AllowAllAzureServicesAndResourcesWithinAzureIps`:

```
Get-AzPostgreSqlFlexibleServerFirewallRule -ResourceGroupName <resourceGroup>
-ServerName <serverName>
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 5e1de0e3-42cb-4ebc-a86d-61d0c619ca48 **- Name:** 'Public network access should be disabled for PostgreSQL flexible servers'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for PostgreSQL flexible servers`.
3. For each database, under `Settings`, click `Networking`.
4. Under `Firewall rules`, uncheck `Allow public access from any Azure service within Azure to this server`.
5. Click `Save`.

Remediate from Azure CLI

Using the firewall rule name from the `Audit from Azure CLI` steps, use the below command to delete the `AllowAllAzureServicesAndResourcesWithinAzureIps` rule for PostgreSQL flexible server:

```
az postgres flexible-server firewall-rule delete --resource-group
<resourceGroup> --name <serverName> --rule-name <ruleName>
```

Type `y` and press `enter` to confirm.

Remediate from PowerShell

Using the firewall rule name from the `Audit from PowerShell` steps, use the below command to delete the `AllowAllAzureServicesAndResourcesWithinAzureIps` rule for PostgreSQL flexible server:

```
Remove-AzPostgreSqlFlexibleServerFirewallRule -ResourceGroupName
<resourceGroup> -ServerName <serverName> -Name <ruleName>
```

Default Value:

The Azure Postgres firewall is set to block all access by default.

References:

1. https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/concepts-firewall-rules
2. https://learn.microsoft.com/en-us/azure/postgresql/flexible-server/how-to-manage-firewall-cli
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-1-establish-network-segmentation-boundaries
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-6-deploy-web-application-firewall

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●

5.2.6 [LEGACY] Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL single server (Automated)

Profile Applicability:

- Level 1

Description:

Enable `log_connections` on `PostgreSQL single servers`.

NOTE: This recommendation currently only applies to Single Server, not Flexible Server. See additional information below for details about the planned retirement of Azure PostgreSQL Single Server.

Rationale:

Enabling `log_connections` helps PostgreSQL Database to log attempted connection to the server, as well as successful completion of client authentication. Log data can be used to identify, troubleshoot, and repair configuration errors and suboptimal performance.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for PostgreSQL servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `log_connections`.
5. Ensure that `log_connections` is set to `ON`.

Audit from Azure CLI
Ensure the below command returns a `Value` of `on`:

```
az postgres server configuration show --resource-group <resourceGroup> --
server-name <serverName> --name log_connections
```

Audit from PowerShell
Ensure the below command returns a `Value` of `on`:

```
Get-AzPostgreSqlConfiguration -ResourceGroupName <resourceGroup> -ServerName
<serverName> -Name log_connections
```

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** eb6f77b9-bd53-4e35-a23d-7f65d5f0e442 **- Name:** 'Log connections should be enabled for PostgreSQL database servers'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for PostgreSQL servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `log_connections`.
5. Set `log_connections` to `ON`.
6. Click `Save`.

Remediate from Azure CLI

Use the below command to update `log_connections` configuration.

```
az postgres server configuration set --resource-group <resourceGroupName> --
server-name <serverName> --name log_connections --value on
```

Remediate from PowerShell

Use the below command to update `log_connections` configuration.

```
Update-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -
ServerName <ServerName> -Name log_connections -Value on
```

Default Value:

By default `log_connections` is enabled (set to `on`).

References:

1. https://docs.microsoft.com/en-us/rest/api/postgresql/configurations/listbyserver
2. https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
4. https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlconfiguration?view=azps-9.2.0#example-2-get-specified-postgresql-configuration-by-name
5. https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlconfiguration?view=azps-9.2.0#example-1-update-postgresql-configuration-by-name

Additional Information:

RETIREMENT of Azure PostgreSQL Single Server: Azure PostgreSQL Single Server is slated for retirement by March 25, 2025. Please use these resources to consider and prepare for migration:

- https://learn.microsoft.com/en-us/azure/postgresql/single-server/whats-happening-to-postgresql-single-server
- https://learn.microsoft.com/en-us/azure/postgresql/migrate/concepts-single-to-flexible

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.2.7 [LEGACY] Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL single server (Automated)

Profile Applicability:

- Level 1

Description:

Enable `log_disconnections` on `PostgreSQL Servers`.

NOTE: This recommendation currently only applies to Single Server, not Flexible Server. See additional information below for details about the planned retirement of Azure PostgreSQL Single Server.

Rationale:

Enabling `log_disconnections` helps PostgreSQL Database to `Logs end of a session`, including duration, which in turn generates query and error logs. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

Impact:

Enabling this setting will enable a log of all disconnections. If this is enabled for a high traffic server, the log may grow exponentially.

Audit:

Audit from Azure Portal

1. From Azure Home select the Portal Menu.
2. Go to `Azure Database` for `PostgreSQL servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. Search for `log_disconnections`.
5. Ensure that `log_disconnections` is set to `ON`.

Audit from Azure CLI

Ensure `log_disconnections` value is set to `ON`

```
az postgres server configuration show --resource-group <resourceGroupName> --
server-name <serverName> --name log_disconnections
```

Audit from PowerShell

Ensure `log_disconnections` value is set to `ON`

```
Get-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -
ServerName <ServerName> -Name log_disconnections
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** eb6f77b9-bd53-4e35-a23d-7f65d5f0e446 **- Name:** 'Disconnections should be logged for PostgreSQL database servers.'

Remediation:

Remediate from Azure Portal

1. From Azure Home select the Portal Menu.
2. Go to `Azure Database` for `PostgreSQL servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. Search for `log_disconnections`.
5. Set `log_disconnections` to `ON`.
6. Click `Save`.

Remediate from Azure CLI

Use the below command to update `log_disconnections` configuration.

```
az postgres server configuration set --resource-group <resourceGroupName> --
server-name <serverName> --name log_disconnections --value on
```

Remediate from PowerShell

Use the below command to update `log_disconnections` configuration.

```
Update-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -
ServerName <ServerName> -Name log_disconnections -Value on
```

Default Value:

By default `log_disconnections` is disabled (set to `off`).

References:

1. https://docs.microsoft.com/en-us/rest/api/postgresql/singleserver/configurations/list-by-server
2. https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
4. https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlconfiguration?view=azps-9.2.0#example-2-get-specified-postgresql-configuration-by-name
5. https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlconfiguration?view=azps-9.2.0#example-1-update-postgresql-configuration-by-name

Additional Information:

RETIREMENT of Azure PostgreSQL Single Server: Azure PostgreSQL Single Server is slated for retirement by March 25, 2025. Please use these resources to consider and prepare for migration:

- https://learn.microsoft.com/en-us/azure/postgresql/single-server/whats-happening-to-postgresql-single-server
- https://learn.microsoft.com/en-us/azure/postgresql/migrate/concepts-single-to-flexible

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.2.8 [LEGACY] Ensure 'Infrastructure double encryption' for PostgreSQL single server is 'Enabled' (Automated)

Profile Applicability:

- Level 1

Description:

Azure Database for PostgreSQL servers should be created with 'infrastructure double encryption' enabled.

NOTE: This recommendation currently only applies to Single Server, not Flexible Server. See additional information below for details about the planned retirement of Azure PostgreSQL Single Server.

Rationale:

If Double Encryption is enabled, another layer of encryption is implemented at the hardware level before the storage or network level. Information will be encrypted before it is even accessed, preventing both interception of data in motion if the network layer encryption is broken and data at rest in system resources such as memory or processor cache. Encryption will also be in place for any backups taken of the database, so the key will secure access the data in all forms. For the most secure implementation of key based encryption, it is recommended to use a Customer Managed asymmetric RSA 2048 Key in Azure Key Vault.

Impact:

The read and write speeds to the database will be impacted if both default encryption and Infrastructure Encryption are checked, as a secondary form of encryption requires more resource overhead for the cryptography of information. This cost is justified for information security. Customer managed keys are recommended for the most secure implementation, leading to overhead of key management. The key will also need to be backed up in a secure location, as loss of the key will mean loss of the information in the database.

Audit:

Audit from Azure Portal

1. From Azure Home, click on more services.
2. Click on `Databases`.
3. Click on `Azure Database for PostgreSQL servers`.
4. Select the database by clicking on its name.
5. Under Security, click Data encryption.
6. Ensure that `Infrastructure encryption enabled` is displayed and is checked.

Audit from Azure CLI

1. Enter the command

```
az postgres server configuration show --name <servername> --resource-group
<resourcegroup> --query 'properties.infrastructureEncryption' -o tsv
```

2. Verify that Infrastructure encryption is enabled.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 24fba194-95d6-48c0-aea7-f65bf859c598 **- Name:** 'Infrastructure encryption should be enabled for Azure Database for PostgreSQL servers'

Remediation:

It is not possible to enable 'infrastructure double encryption' on an existing Azure Database for PostgreSQL server.
The remediation steps detail the creation of a new Azure Database for PostgreSQL server with 'infrastructure double encryption' enabled.
Remediate from Azure Portal

1. Go through the normal process of database creation.
2. On step 2 titled `Additional settings` ensure that `Infrastructure double encryption enabled` is checked.
3. Acknowledge that you understand this will impact database performance.
4. Finish database creation as normal.

Remediate from Azure CLI

```
az postgres server create --resource-group <resourcegroup> --name
<servername>  --location <location> --admin-user <adminusername> --admin-
password <server_admin_password> --sku-name GP_Gen4_2 --version 11 --
infrastructure-encryption Enabled
```

Default Value:

By Default, Double Encryption is disabled.

References:

1. https://docs.microsoft.com/en-us/azure/postgresql/howto-double-encryption
2. https://docs.microsoft.com/en-us/azure/postgresql/concepts-infrastructure-double-encryption

3. https://docs.microsoft.com/en-us/azure/postgresql/concepts-data-encryption-postgresql
4. https://docs.microsoft.com/en-us/azure/key-vault/keys/byok-specification
5. https://docs.microsoft.com/en-us/azure/postgresql/howto-double-encryption
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-4-enable-data-at-rest-encryption-by-default

Additional Information:

RETIREMENT of Azure PostgreSQL Single Server: Azure PostgreSQL Single Server is slated for retirement by March 25, 2025. Please use these resources to consider and prepare for migration:

- https://learn.microsoft.com/en-us/azure/postgresql/single-server/whats-happening-to-postgresql-single-server
- https://learn.microsoft.com/en-us/azure/postgresql/migrate/concepts-single-to-flexible

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

5.3 Azure Database for MySQL

This section covers security best practice recommendations for Azure MySQL Database Servers.

Azure Product Page: https://azure.microsoft.com/en-us/products/mysql/

RETIREMENT of Azure MySQL Single Server: Azure MySQL Single Server is slated for retirement by September 16, 2024. Azure MySQL Flexible Server is the newer deployment standard and is unaffected. Please use these resources to consider and prepare for migration:

- https://learn.microsoft.com/en-us/azure/mysql/migrate/whats-happening-to-mysql-single-server
- https://learn.microsoft.com/en-us/azure/mysql/migrate/how-to-decide-on-right-migration-tools

5.3.1 Ensure server parameter 'require_secure_transport' is set to 'ON' for MySQL flexible server (Automated)

Profile Applicability:

- Level 1

Description:

Enable require_secure_transport on MySQL flexible servers.

Rationale:

SSL connectivity helps to provide a new layer of security by connecting database server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between database server and client applications helps protect against "man in the middle" attacks by encrypting the data stream between the server and application.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to Azure Database for MySQL flexible servers.
3. For each database, under Settings, click Server parameters.
4. In the filter bar, type require_secure_transport.
5. Ensure that the VALUE for require_secure_transport is ON.

Audit from Azure CLI

Ensure the below command returns a value of on:

```
az mysql flexible-server parameter show --resource-group <resourceGroup> --
server-name <serverName> --name require_secure_transport
```

Audit from PowerShell

Ensure the below command returns a Value of on:

```
Get-AzMySqlFlexibleServerConfiguration -ResourceGroupName <resourceGroup> -
ServerName <serverName> -Name require_secure_transport
```

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to Azure Database for MySQL flexible servers.
3. For each database, under Settings, click Server parameters.
4. In the filter bar, type require_secure_transport.
5. Set the VALUE for require_secure_transport to ON.
6. Click Save.

Remediate from Azure CLI

Use the below command to enable `require_secure_transport`:

```
az mysql flexible-server parameter set --resource-group <resourceGroup> --
server-name <serverName> --name require_secure_transport --value on
```

Remediate from PowerShell

Use the below command to enable `require_secure_transport`:

```
Update-AzMySqlFlexibleServerConfiguration -ResourceGroupName <resourceGroup>
-ServerName <serverName> -Name require_secure_transport -Value on
```

Default Value:

Azure Database for MySQL when provisioned through the Azure portal or CLI will require SSL connections by default.

References:

1. https://learn.microsoft.com/en-us/azure/mysql/flexible-server/concepts-networking#tls-and-ssl
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

5.3.2 Ensure server parameter 'tls_version' is set to 'TLSv1.2' (or higher) for MySQL flexible server (Automated)

Profile Applicability:

- Level 1

Description:

Ensure `tls_version` on `MySQL flexible servers` is set to use TLS version 1.2 or higher.

Rationale:

TLS connectivity helps to provide a new layer of security by connecting database server to client applications using Transport Layer Security (TLS). Enforcing TLS connections between database server and client applications helps protect against "man in the middle" attacks by encrypting the data stream between the server and application.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for MySQL flexible servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `tls_version`.
5. Ensure `tls_version` is set to `TLSv1.2` (or higher).

Audit from PowerShell

Ensure the `Value` of the below command contains `TLSv1.2` or higher, and does not contain anything lower than `TLSv1.2`:

```
Get-AzMySqlFlexibleServerConfiguration -ResourceGroupName <resourceGroup> -
ServerName <ServerName> -Name tls_version
```

Audit from Azure CLI

Ensure the `value` of the below command contains `TLSv1.2` or higher, and does not contain anything lower than `TLSv1.2`:

```
az mysql flexible-server parameter show --resource-group <resourceGroup> --
server-name <serverName> --name tls_version
```

Example output – next page

```
{
  "allowedValues": "TLSv1,TLSv1.1,TLSv1.2",
  "dataType": "Set",
  "defaultValue": "TLSv1.2",
  "description": "Which protocols the server permits for encrypted
connections. By default, TLS 1.2 is enforced",
  "id":
"/subscriptions/<subscriptionId>/resourceGroups/<resourceGroupName>/providers
/Microsoft.DBforMySQL/flexibleServers/<serverName>/configurations/tls_version
",
  "isConfigPendingRestart": "False",
  "isDynamicConfig": "False",
  "isReadOnly": "False",
  "name": "tls_version",
  "resourceGroup": "<resourceGroupName>",
  "source": "system-default",
  "systemData": null,
  "type": "Microsoft.DBforMySQL/flexibleServers/configurations",
  "value": "TLSv1.2"
}
```

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for MySQL flexible servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `tls_version`.
5. Click on the VALUE dropdown next to `tls_version`, and check `TLSv1.2` (or higher).
6. Uncheck anything lower than `TLSv1.2`.
7. Click `Save`.

Remediate from Azure CLI

Use the below command to update MySQL flexible servers to use TLS version 1.2:

```
az mysql flexible-server parameter set --resource-group <resourceGroup> --
server-name <serverName> --name tls_version --value TLSv1.2
```

Remediate from PowerShell

Use the below command to update MySQL flexible servers to use TLS version 1.2:

```
Update-AzMySqlFlexibleServerConfiguration -ResourceGroupName <resourceGroup>
-ServerName <serverName> -Name tls_version -Value TLSv1.2
```

Default Value:

By default, TLS is set to v1.2 for MySQL Flexible servers.

References:

1. https://learn.microsoft.com/en-us/azure/mysql/flexible-server/concepts-networking#tls-and-ssl
2. https://learn.microsoft.com/en-us/azure/mysql/flexible-server/how-to-connect-tls-ssl
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

5.3.3 Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL flexible server (Automated)

Profile Applicability:

- Level 2

Description:

Enable `audit_log_enabled` on `MySQL flexible servers`.

Rationale:

Enabling `audit_log_enabled` helps MySQL Database to log items such as connection attempts to the server, DDL/DML access, and more. Log data can be used to identify, troubleshoot, and repair configuration errors and suboptimal performance.

Impact:

There are further costs incurred for storage of logs. For high traffic databases these logs will be significant. Determine your organization's needs before enabling.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for MySQL Servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `audit_log_enabled`.
5. Ensure that the `VALUE` for `audit_log_enabled` is `ON`.

Audit from Azure CLI
Ensure the below command returns a `value` of `on`:

```
az mysql flexible-server parameter show --resource-group <resourceGroup> --
server-name <serverName> --name audit_log_enabled
```

Audit from PowerShell
Ensure the below command returns a `Value` of `on`:

```
Get-AzMySqlFlexibleServerConfiguration -ResourceGroupName <resourceGroup> -
ServerName <serverName> -Name audit_log_enabled
```

Remediation:

Remediate from Azure Portal
Part 1 - Turn on audit logs

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for MySQL flexible servers`.

3. For each database, under `Settings`, click `Server parameters`.
4. Set `audit_log_enabled` to `ON`.
5. Click `Save`.

Part 2 - Capture audit logs (diagnostic settings is for example only, send these logs to the appropriate data sink for your logging needs)

1. Under Monitoring, select `Diagnostic settings`.
2. Select `+ Add diagnostic setting`.
3. Provide a diagnostic setting name.
4. Under Categories, select `MySQL Audit Logs`.
5. Specify destination details.
6. Click `Save`.

It may take up to 10 minutes for the logs to appear in the configured destination.

Remediate from Azure CLI
Use the below command to enable `audit_log_enabled` :

```
az mysql flexible-server parameter set --resource-group <resourceGroup> --
server-name <serverName> --name audit_log_enabled --value on
```

Remediate from PowerShell
Use the below command to enable `audit_log_enabled` :

```
Update-AzMySqlFlexibleServerConfiguration -ResourceGroupName <resourceGroup>
-ServerName <serverName> -Name audit_log_enabled -Value on
```

Default Value:

audit_log_enabled is set to OFF by default

References:

1. https://learn.microsoft.com/en-us/azure/mysql/flexible-server/tutorial-configure-audit
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
3. https://learn.microsoft.com/en-us/azure/mysql/flexible-server/tutorial-configure-audit#configure-auditing-by-using-the-azure-cli

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.3.4 Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL flexible server (Automated)

Profile Applicability:

- Level 2

Description:

Set `audit_log_events` to include `CONNECTION` on `MySQL flexible servers`.

Rationale:

Enabling `CONNECTION` helps MySQL Database to log items such as successful and failed connection attempts to the server. Log data can be used to identify, troubleshoot, and repair configuration errors and suboptimal performance.

Impact:

There are further costs incurred for storage of logs. For high traffic databases these logs will be significant. Determine your organization's needs before enabling.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for MySQL flexible servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `audit_log`.
5. Ensure that the `VALUE` for `audit_log_enabled` is `ON`.
6. Ensure that the `VALUE` for `audit_log_events` includes `CONNECTION`.

Audit from Azure CLI

Ensure the below command returns a `value` that includes `CONNECTION`:

```
az mysql flexible-server parameter show --resource-group <resourceGroup> --
server-name <serverName> --name audit_log_events
```

Audit from PowerShell

Ensure the below command returns a `Value` that includes `CONNECTION`:

```
Get-AzMySqlFlexibleServerConfiguration -ResourceGroupName <resourceGroup> -
ServerName <serverName> -Name audit_log_events
```

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com.
2. Go to `Azure Database for MySQL flexible servers`.
3. For each database, under `Settings`, click `Server parameters`.
4. In the filter bar, type `audit_log`.
5. Set `audit_log_enabled` to `ON`.
6. In the drop-down next to `audit_log_events`, check `CONNECTION`.
7. Click `Save`.
8. Under `Monitoring`, select `Diagnostic settings`.
9. Select `+ Add diagnostic setting`.
10. Provide a diagnostic setting name.
11. Under `Categories`, select `MySQL Audit Logs`.
12. Specify destination details.
13. Click `Save`.

It may take up to 10 minutes for the logs to appear in the configured destination.

Remediate from Azure CLI

Use the below command to set `audit_log_events` to `CONNECTION`:

```
az mysql flexible-server parameter set --resource-group <resourceGroup> --
server-name <serverName> --name audit_log_events --value CONNECTION
```

Remediate from PowerShell

Use the below command to set `audit_log_events` to `CONNECTION`:

```
Update-AzMySqlFlexibleServerConfiguration -ResourceGroupName <resourceGroup>
-ServerName <serverName> -Name audit_log_events -Value CONNECTION
```

Default Value:

By default `audit_log_events` is set to `CONNECTION`.

References:

1. https://learn.microsoft.com/en-us/azure/mysql/flexible-server/concepts-audit-logs
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
3. https://learn.microsoft.com/en-us/azure/mysql/flexible-server/tutorial-configure-audit
4. https://learn.microsoft.com/en-us/azure/mysql/flexible-server/tutorial-configure-audit#configure-auditing-by-using-the-azure-cli

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

5.4 Azure Cosmos DB

This section covers security best practice recommendations for Azure Cosmos DB Database Servers.

Azure Product Page: https://azure.microsoft.com/en-us/products/cosmos-db/

5.4.1 Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks (Automated)

Profile Applicability:

- Level 2

Description:

Limiting your Cosmos DB to only communicate on whitelisted networks lowers its attack footprint.

Rationale:

Selecting certain networks for your Cosmos DB to communicate restricts the number of networks including the internet that can interact with what is stored within the database.

Impact:

WARNING: Failure to whitelist the correct networks will result in a connection loss.

WARNING: Changes to Cosmos DB firewalls may take up to 15 minutes to apply. Ensure that sufficient time is planned for remediation or changes to avoid disruption.

Audit:

Audit from Azure Portal

1. Open the portal menu.
2. Select the Azure Cosmos DB blade
3. Select a Cosmos DB to audit.
4. Select `Networking`.
5. Under `Public network access`, ensure `Selected networks` is selected.
6. Under `Virtual networks`, ensure appropriate virtual networks are configured.

Audit from Azure CLI

Retrieve a list of all CosmosDB database names:

```
az cosmosdb list
```

For each database listed, run the following command:

```
az cosmosdb show <database id>
```

For each database, ensure that `isVirtualNetworkFilterEnabled` is set to `true`

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 862e97cf-49fc-4a5c-9de4-40d4e2e7c8eb **- Name:** 'Azure Cosmos DB accounts should have firewall rules'

Remediation:

Remediate from Azure Portal

1. Open the portal menu.
2. Select the Azure Cosmos DB blade.
3. Select a Cosmos DB account to audit.
4. Select `Networking`.
5. Under `Public network access`, select `Selected networks`.
6. Under `Virtual networks`, select `+ Add existing virtual network` or `+ Add a new virtual network`.
7. For existing networks, select subscription, virtual network, subnet and click `Add`. For new networks, provide a name, update the default values if required, and click `Create`.
8. Click `Save`.

Default Value:

By default, Cosmos DBs are set to have access all networks.

References:

1. https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints
2. https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-vnet-service-endpoint
3. https://docs.microsoft.com/en-us/cli/azure/cosmosdb?view=azure-cli-latest#az-cosmosdb-show
4. https://docs.microsoft.com/en-us/cli/azure/cosmosdb/database?view=azure-cli-latest#az-cosmosdb-database-list
5. https://docs.microsoft.com/en-us/powershell/module/az.cosmosdb/?view=azps-8.1.0
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	9.4 Apply Host-based Firewalls or Port Filtering Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v7	14.1 Segment the Network Based on Sensitivity Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).		●	●

5.4.2 Ensure That Private Endpoints Are Used Where Possible (Automated)

Profile Applicability:

- Level 2

Description:

Private endpoints limit network traffic to approved sources.

Rationale:

For sensitive data, private endpoints allow granular control of which services can communicate with Cosmos DB and ensure that this network traffic is private. You set this up on a case by case basis for each service you wish to be connected.

Impact:

Only whitelisted services will have access to communicate with the Cosmos DB.

Audit:

Audit from Azure Portal

1. Open the portal menu.
2. Select the Azure Cosmos DB blade.
3. Select the Azure Cosmos DB account.
4. Select `Networking`.
5. Ensure `Public network access` is set to `Selected networks`.
6. Ensure the listed networks are set appropriately.
7. Select `Private access`.
8. Ensure a private endpoint exists and `Connection state` is `Approved`.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 58440f8a-10c5-4151-bdce-dfbaad4a20b7 **- Name:** 'CosmosDB accounts should use private link'

Remediation:

Remediate from Azure Portal

1. Open the portal menu.
2. Select the Azure Cosmos DB blade.

3. Select the Azure Cosmos DB account.
4. Select `Networking`.
5. Select `Private access`.
6. Click `+ Private Endpoint`.
7. Provide a Name.
8. Click `Next`.
9. From the Resource type drop down, select `Microsoft.AzureCosmosDB/databaseAccounts`.
10. From the Resource drop down, select the Cosmos DB account.
11. Click `Next`.
12. Provide appropriate Virtual Network details.
13. Click `Next`.
14. Provide appropriate DNS details.
15. Click `Next`.
16. Optionally provide Tags.
17. Click `Next : Review + create`.
18. Click `Create`.

Default Value:

By default Cosmos DB does not have private endpoints enabled and its traffic is public to the network.

References:

1. https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints
2. https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-cosmosdb-portal
3. https://docs.microsoft.com/en-us/cli/azure/cosmosdb/private-endpoint-connection?view=azure-cli-latest
4. https://docs.microsoft.com/en-us/cli/azure/network/private-endpoint?view=azure-cli-latest#az-network-private-endpoint-create
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-2-secure-cloud-native-services-with-network-controls

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	14.1 Segment the Network Based on Sensitivity Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).		●	●

5.4.3 Use Entra ID Client Authentication and Azure RBAC where possible (Manual)

Profile Applicability:

- Level 1

Description:

Cosmos DB can use tokens or Entra ID for client authentication which in turn will use Azure RBAC for authorization. Using Entra ID is significantly more secure because Entra ID handles the credentials and allows for MFA and centralized management, and the Azure RBAC is better integrated with the rest of Azure.

Rationale:

Entra ID client authentication is considerably more secure than token-based authentication because the tokens must be persistent at the client. Entra ID does not require this.

Audit:

Audit from PowerShell

```
$cosmosdbname = "<your-cosmos-db-account-name>"
$resourcegroup = "<your-resource-group-name>"
az cosmosdb show --name $cosmosdbname --resource-group $resourcegroup |
ConvertFrom-Json
```

In the resulting output, disableLocalAuth should be true
Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 5450f5bd-9c72-4390-a9c4-a7aba4edfdd2 **- Name:** 'Cosmos DB database accounts should have local authentication methods disabled'

Remediation:

Map all the resources that currently have access to the Azure Cosmos DB account with keys or access tokens.
Create an Entra ID identity for each of these resources:

- For Azure resources, you can create a managed identity. You may choose between system-assigned and user-assigned managed identities.
- For non-Azure resources, create an Entra ID identity. Grant each Entra ID identity the minimum permission it requires. When possible, we recommend you

use one of the 2 built-in role definitions: Cosmos DB Built-in Data Reader or Cosmos DB Built-in Data Contributor. Validate that the new resource is functioning correctly. After new permissions are granted to identities, it may take a few hours until they propagate. When all resources are working correctly with the new identities, continue to the next step.

Remediate from PowerShell

```
$cosmosdbname = "<your-cosmos-db-account-name>"
$resourcegroup = "<your-resource-group-name>"
az cosmosdb show --name $cosmosdbname --resource-group $resourcegroup |
ConvertFrom-Json
az resource update --ids $cosmosdb.id --set properties.disableLocalAuth=true
--latest-include-preview
```

Default Value:

The default is to use tokens/keys for client authentication.

References:

1. https://learn.microsoft.com/en-us/azure/cosmos-db/role-based-access-control

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.7 Centralize Access Control Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

6 Logging and Monitoring

This section covers security recommendations to follow for logging and monitoring policies on an Azure Subscription.

Scoping: A necessary exercise for effective and efficient use of Logging and Monitoring

For recommendations contained in this section, it is crucial that your organization consider and settle on the scope of application for each recommendation individually. The scope of application cannot be realistically written in a generic prescriptive way within these recommendations, so a scoping exercise is strongly recommended. A scoping exercise will help you determine which resources are "in scope" and will receive partial or complete logging and monitoring treatment, and which resources are "out of scope" and will not receive any logging and monitoring treatment.

Your objectives with the scoping exercise should be to:

- Produce a clear classification of resources
- Understand the control requirements of any relevant security or compliance frameworks
- Ensure the appropriate personnel can detect and react to threats
- Ensure relevant resources have a historical register for accountability and investigation
- Minimize alert fatigue and cost

Release Environments provide a helpful context for understanding scope from a DevOps perspective. For example:

1. Production Environment
2. Staging Environment
3. Testing Environment
4. Development Environment

While resources considered in the scope of a Production Environment might have a full set of recommendations applied for logging and monitoring, other release environments might have a limited set of recommendations applied for the sake of accountability. The names of these environments and which resources are in the scope of each environment will vary from one organization to another.

6.1 Configuring Diagnostic Settings

The Azure Diagnostic Settings capture control/management activities performed on a subscription or Azure AD Tenant. By default, the Azure Portal retains activity logs only for 90 days. The Diagnostic Settings define the type of events that are stored or streamed and the outputs—storage account, log analytics workspace, event hub, and others. The Diagnostic Settings, if configured properly, can ensure that all logs are retained for longer duration. This section has recommendations for correctly configuring the Diagnostic Settings so that all logs captured are retained for longer periods.

Azure Subscriptions

When configuring Diagnostic Settings, you may choose to export in one of four ways in which you need to ensure appropriate data retention. The options are Log Analytics workspace, Event Hub, Storage Account, and Partner Solutions. It is important to ensure you are aware and have set retention as your organization sees fit.

Azure AD Logs

In order to retain sign in logs, user account changes, application provisioning logs, or other logs that are visible to only on the Tenant in Azure AD, separate Diagnostic settings must be specified.

Deployment by Policy

Deploying Azure diagnostics should ideally be done by policy to ensure a consistent configuration, Microsoft provide a full set of policies for all diagnostic capable resource types in their github repository. If you chose to deploy by policy, it is best to route the diagnostics to a Log Analytics Workspace so that they can be used in Azure Monitor or Azure Sentinel. Be aware that this has a cost attached to it. Future versions of the CIS Azure Foundations Benchmark will aim to cover the use of policy in greater detail.

6.1.1 Ensure that a 'Diagnostic Setting' exists for Subscription Activity Logs (Manual)

Profile Applicability:

- Level 1

Description:

Enable Diagnostic settings for exporting activity logs. Diagnostic settings are available for each individual resource within a subscription. Settings should be configured for all appropriate resources for your environment.

Rationale:

A diagnostic setting controls how a diagnostic log is exported. By default, logs are retained only for 90 days. Diagnostic settings should be defined so that logs can be exported and stored for a longer duration in order to analyze security activities within an Azure subscription.

Audit:

Audit from Azure Portal
To identify Diagnostic Settings on a subscription:

1. Go to `Monitor`
2. Click `Activity Log`
3. Click `Export Activity Logs`
4. Select a `Subscription`
5. Ensure a `Diagnostic setting` exists for the selected Subscription

To identify Diagnostic Settings on specific resources:

1. Go to `Monitoring`
2. Click `Diagnostic settings`
3. Ensure a `Diagnostic setting` exists for all appropriate resources.

Audit from Azure CLI
To identify Diagnostic Settings on a subscription:

```
az monitor diagnostic-settings subscription list --subscription <subscription
ID>
```

To identify Diagnostic Settings on a resource

```
az monitor diagnostic-settings list --resource <resource Id>
```

Audit from PowerShell

To identify Diagnostic Settings on a Subscription:

```
Get-AzDiagnosticSetting -SubscriptionId <subscription ID>
```

To identify Diagnostic Settings on a specific resource:

```
Get-AzDiagnosticSetting -ResourceId <resource ID>
```

Remediation:

Remediate from Azure Portal

To enable Diagnostic Settings on a Subscription:

1. Go to `Monitor`
2. Click on `Activity log`
3. Click on `Export Activity Logs`
4. Click `+ Add diagnostic setting`
5. Enter a `Diagnostic setting name`
6. Select `Categories` for the diagnostic setting
7. Select the appropriate `Destination details` (this may be Log Analytics, Storage Account, Event Hub, or Partner solution)
8. Click `Save`

To enable Diagnostic Settings on a specific resource:

1. Go to `Monitoring`
2. Click `Diagnostic settings`
3. Select `Add diagnostic setting`
4. Enter a `Diagnostic setting name`
5. Select the appropriate log, metric, and destination (this may be Log Analytics, Storage Account, Event Hub, or Partner solution)
6. Click `Save`

Repeat these step for all resources as needed.

Remediate from Azure CLI

To configure Diagnostic Settings on a Subscription:

```
az monitor diagnostic-settings subscription create --subscription
<subscription id> --name <diagnostic settings name> --location <location> <[-
-event-hub <event hub ID> --event-hub-auth-rule <event hub auth rule ID>] [--
storage-account <storage account ID>] [--workspace <log analytics workspace
ID>] --logs "<JSON encoded categories>" (e.g.
[{category:Security,enabled:true},{category:Administrative,enabled:true},{cat
egory:Alert,enabled:true},{category:Policy,enabled:true}])
```

To configure Diagnostic Settings on a specific resource:

```
az monitor diagnostic-settings create --subscription <subscription ID> --
resource <resource ID> --name <diagnostic settings name> <[--event-hub <event
hub ID> --event-hub-rule <event hub auth rule ID>] [--storage-account
<storage account ID>] [--workspace <log analytics workspace ID>] --logs
<resource specific JSON encoded log settings> --metrics <metric settings
(shorthand|json-file|yaml-file)>
```

Remediate from PowerShell

To configure Diagnostic Settings on a subscription:

```
$logCategories = @();
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Administrative -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Security -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category ServiceHealth -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Alert -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Recommendation -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Policy -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Autoscale -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category ResourceHealth -Enabled $true

New-AzSubscriptionDiagnosticSetting -SubscriptionId <subscription ID> -Name
<Diagnostic settings name> <[-EventHubAuthorizationRule <event hub auth rule
ID> -EventHubName <event hub name>] [-StorageAccountId <storage account ID>]
[-WorkSpaceId <log analytics workspace ID>] [-MarketplacePartner ID <full ARM
Marketplace resource ID>]> -Log $logCategories
```

To configure Diagnostic Settings on a specific resource:

```
$logCategories = @()
$logCategories +=  New-AzDiagnosticSettingLogSettingsObject -Category
<resource specific log category> -Enabled $true

Repeat command and variable assignment for each Log category specific to the
resource where this Diagnostic Setting will get configured.


$metricCategories = @()
$metricCategories += New-AzDiagnosticSettingMetricSettingsObject -Enabled
$true [-Category <resource specific metric category | AllMetrics>] [-
RetentionPolicyDay <Integer>] [-RetentionPolicyEnabled $true]

Repeat command and variable assignment for each Metric category or use the
'AllMetrics' category.


New-AzDiagnosticSetting -ResourceId <resource ID> -Name <Diagnostic settings
name> -Log $logCategories -Metric $metricCategories [-
EventHubAuthorizationRuleId <event hub auth rule ID> -EventHubName <event hub
name>] [-StorageAccountId <storage account ID>] [-WorkspaceId <log analytics
workspace ID>] [-MarketplacePartnerId <full ARM marketplace resource ID>]>
```

Default Value:

By default, diagnostic setting is not set.

References:

1. https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs#export-the-activity-log-with-a-log-profile
2. https://learn.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?view=azure-cli-latest
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

6.1.2 Ensure Diagnostic Setting captures appropriate categories (Automated)

Profile Applicability:

- Level 1

Description:

Prerequisite: A Diagnostic Setting must exist. If a Diagnostic Setting does not exist, the navigation and options within this recommendation will not be available. Please review the recommendation at the beginning of this subsection titled: "Ensure that a 'Diagnostic Setting' exists."

The diagnostic setting should be configured to log the appropriate activities from the control/management plane.

Rationale:

A diagnostic setting controls how the diagnostic log is exported. Capturing the diagnostic setting categories for appropriate control/management plane activities allows proper alerting.

Audit:

Audit from Azure Portal

1. Go to `Monitor`.
2. Click `Activity log`.
3. Click on `Export Activity Logs`.
4. Select the appropriate `Subscription`.
5. Click `Edit setting` next to a diagnostic setting.
6. Ensure that the following categories are checked: `Administrative, Alert, Policy, and Security`.

Audit from Azure CLI
Ensure the categories `'Administrative', 'Alert', 'Policy', and 'Security'` set to: 'enabled: true'

```
az monitor diagnostic-settings subscription list --subscription <subscription
ID>
```

Audit from PowerShell
Ensure the categories Administrative, Alert, Policy, and Security are set to Enabled:True

```
Get-AzSubscriptionDiagnosticSetting -Subscription <subscriptionID>
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 3b980d31-7904-4bb7-8575-5665739a8052 **- Name:** 'An activity log alert should exist for specific Security operations'
- **Policy ID:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'
- **Policy ID:** c5447c04-a4d7-4ba8-a263-c9ee321a6858 **- Name:** 'An activity log alert should exist for specific Policy operations'

Remediation:

Remediate from Azure Portal

1. Go to `Monitor`.
2. Click `Activity log`.
3. Click on `Export Activity Logs`.
4. Select the `Subscription` from the drop down menu.
5. Click `Edit setting` next to a diagnostic setting.
6. Check the following categories: `Administrative, Alert, Policy, and Security`.
7. Choose the destination details according to your organization's needs.
8. Click `Save`.

Remediate from Azure CLI

```
az monitor diagnostic-settings subscription create --subscription
<subscription id> --name <diagnostic settings name> --location <location> <[-
-event-hub <event hub ID> --event-hub-auth-rule <event hub auth rule ID>] [--
storage-account <storage account ID>] [--workspace <log analytics workspace
ID>] --logs
"[{category:Security,enabled:true},{category:Administrative,enabled:true},{ca
tegory:Alert,enabled:true},{category:Policy,enabled:true}]"
```

Remediate from PowerShell

```
$logCategories = @();
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Administrative -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Security -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Alert -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Policy -Enabled $true

New-AzSubscriptionDiagnosticSetting -SubscriptionId <subscription ID> -Name
<Diagnostic settings name> <[-EventHubAuthorizationRule <event hub auth rule
ID> -EventHubName <event hub name>] [-StorageAccountId <storage account ID>]
[-WorkSpaceId <log analytics workspace ID>] [-MarketplacePartner ID <full ARM
Marketplace resource ID>]> -Log $logCategories
```

Default Value:

When the diagnostic setting is created using Azure Portal, by default no categories are selected.

References:

1. https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings
2. https://docs.microsoft.com/en-us/azure/azure-monitor/samples/resource-manager-diagnostic-settings
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
4. https://learn.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?view=azure-cli-latest
5. https://learn.microsoft.com/en-us/powershell/module/az.monitor/new-azsubscriptiondiagnosticsetting?view=azps-9.2.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.1.3 Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (CMK) (Automated)

Profile Applicability:

- Level 2

Description:

Storage accounts with the activity log exports can be configured to use Customer Managed Keys (CMK).

Rationale:

Configuring the storage account with the activity log export container to use CMKs provides additional confidentiality controls on log data, as a given user must have read permission on the corresponding storage account and must be granted decrypt permission by the CMK.

Impact:

NOTE: You must have your key vault setup to utilize this. All Audit Logs will be encrypted with a key you provide. You will need to set up customer managed keys separately, and you will select which key to use via the instructions here. You will be responsible for the lifecycle of the keys, and will need to manually replace them at your own determined intervals to keep the data secure.

Audit:

Audit from Azure Portal

1. Go to `Monitor`.
2. Select `Activity log`.
3. Select `Export Activity Logs`.
4. Select a `Subscription`.
5. Note the name of the `Storage Account` for the diagnostic setting.
6. Navigate to `Storage accounts`.
7. Click on the storage account name noted in Step 5.
8. Under `Security + networking`, click `Encryption`.
9. Ensure `Customer-managed keys` is selected and a key is set.

Audit from Azure CLI

1. Get storage account id configured with log profile:

```
az monitor diagnostic-settings subscription list --subscription <subscription
id> --query 'value[*].storageAccountId'
```

2. Ensure the storage account is encrypted with CMK:

```
az storage account list --query "[?name=='<Storage Account Name>']"
```

In command output ensure `keySource` is set to `Microsoft.Keyvault` and `keyVaultProperties` is not set to `null`

Audit from PowerShell

```
Get-AzStorageAccount -ResourceGroupName <resource group name> -Name <storage
account name>|select-object -ExpandProperty encryption|format-list
```

Ensure the value of `KeyVaultProperties` is not `null` or empty, and ensure `KeySource` is not set to `Microsoft.Storage`.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** fbb99e8e-e444-4da0-9ff1-75c92f5a85b2 **- Name:** 'Storage account containing the container with activity logs must be encrypted with BYOK'

Remediation:

Remediate from Azure Portal

1. Go to `Monitor`.
2. Select `Activity log`.
3. Select `Export Activity Logs`.
4. Select a `Subscription`.
5. Note the name of the `Storage Account` for the diagnostic setting.
6. Navigate to `Storage accounts`.
7. Click on the storage account.
8. Under `Security + networking`, click `Encryption`.
9. Next to `Encryption type`, select `Customer-managed keys`.
10. Complete the steps to configure a customer-managed key for encryption of the storage account.

Remediate from Azure CLI

```
az storage account update --name <name of the storage account> --resource-
group <resource group for a storage account> --encryption-key-
source=Microsoft.Keyvault --encryption-key-vault <Key Vault URI> --
encryption-key-name <KeyName> --encryption-key-version <Key Version>
```

Remediate from PowerShell

```
Set-AzStorageAccount -ResourceGroupName <resource group name> -Name <storage
account name> -KeyvaultEncryption -KeyVaultUri <key vault URI> -KeyName <key
name>
```

Default Value:

By default, for a storage account `keySource` is set to `Microsoft.Storage` allowing encryption with vendor Managed key and not a Customer Managed Key.

References:

1. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required
2. https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log?tabs=cli#managing-legacy-log-profiles

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

6.1.4 Ensure that logging for Azure Key Vault is 'Enabled' (Automated)

Profile Applicability:

- Level 1

Description:

Enable AuditEvent logging for key vault instances to ensure interactions with key vaults are logged and available.

Rationale:

Monitoring how and when key vaults are accessed, and by whom, enables an audit trail of interactions with confidential information, keys, and certificates managed by Azure Key Vault. Enabling logging for Key Vault saves information in a user provided destination of either an Azure storage account or Log Analytics workspace. The same destination can be used for collecting logs for multiple Key Vaults.

Audit:

Audit from Azure Portal

1. Go to `Key vaults`.
2. For each Key vault, under `Monitoring`, go to `Diagnostic settings`.
3. Click `Edit setting` next to a diagnostic setting.
4. Ensure that a destination is configured.
5. Under `Category groups`, ensure that `audit` and `allLogs` are checked.

Audit from Azure CLI

List all key vaults

```
az keyvault list
```

For each keyvault `id`

```
az monitor diagnostic-settings list --resource <id>
```

Ensure that `storageAccountId` reflects your desired destination and that `categoryGroup` and `enabled` are set as follows in the sample outputs below.

```
"logs": [
{
    "categoryGroup": "audit",
    "enabled": true,
},
{
    "categoryGroup": "allLogs",
    "enabled": true,
}
```

Audit from PowerShell
List the key vault(s) in the subscription

```
Get-AzKeyVault
```

For each key vault, run the following:

```
Get-AzDiagnosticSetting -ResourceId <key_vault_id>
```

Ensure that `StorageAccountId`, `ServiceBusRuleId`, `MarketplacePartnerId`, or `WorkspaceId` is set as appropriate. Also, ensure that `enabled` is set to `true`, and that `categoryGroup` reflects both `audit` and `allLogs` category groups.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** cf820ca0-f99e-4f3e-84fb-66e913812d21 **- Name:** 'Resource logs in Key Vault should be enabled'

Remediation:

Remediate from Azure Portal

1. Go to `Key vaults`.
2. Select a Key vault.
3. Under `Monitoring`, select `Diagnostic settings`.
4. Click `Edit setting` to update an existing diagnostic setting, or `Add diagnostic setting` to create a new one.
5. If creating a new diagnostic setting, provide a name.
6. Configure an appropriate destination.
7. Under `Category groups`, check `audit` and `allLogs`.
8. Click `Save`.

Remediate from Azure CLI
To update an existing `Diagnostic Settings`

```
az monitor diagnostic-settings update --name "<diagnostic_setting_name>" --
resource <key_vault_id>
```

To create a new `Diagnostic Settings`

```
az monitor diagnostic-settings create --name "<diagnostic_setting_name>" --
resource <key_vault_id> --logs
"[{category:audit,enabled:true},{category:allLogs,enabled:true}]" --metrics
"[{category:AllMetrics,enabled:true}]" <[--event-hub <event_hub_ID> --event-
hub-rule <event_hub_auth_rule_ID> | --storage-account <storage_account_ID> |-
-workspace <log_analytics_workspace_ID> | --marketplace-partner-id
<solution_resource_ID>]>
```

Remediate from PowerShell

Create the `Log` settings object

```
$logSettings = @()
$logSettings += New-AzDiagnosticSettingLogSettingsObject -Enabled $true -
Category audit
$logSettings += New-AzDiagnosticSettingLogSettingsObject -Enabled $true -
Category allLogs
```

Create the `Metric` settings object

```
$metricSettings = @()
$metricSettings += New-AzDiagnosticSettingMetricSettingsObject -Enabled $true
-Category AllMetrics
```

Create the `Diagnostic Settings` for each `Key Vault`

```
New-AzDiagnosticSetting -Name "<diagnostic_setting_name>" -ResourceId
<key_vault_id> -Log $logSettings -Metric $metricSettings [-StorageAccountId
<storage_account_ID> | -EventHubName <event_hub_name> -
EventHubAuthorizationRuleId <event_hub_auth_rule_ID> | -WorkSpaceId <log
analytics workspace ID> | -MarketPlacePartnerId <full resource ID for third-
party solution>]
```

Default Value:

By default, Diagnostic AuditEvent logging is not enabled for Key Vault instances.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/general/howto-logging
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-8-ensure-security-of-key-and-certificate-repository
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

Additional Information:

DEPRECATION WARNING

Retention rules for Key Vault logging is being migrated to Azure Storage Lifecycle Management. Retention rules should be set based on the needs of your organization and security or compliance frameworks. Please visit https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/migrate-to-azure-storage-lifecycle-policy?tabs=portal for detail on migrating your retention rules.

Microsoft has provided the following deprecation timeline:

March 31, 2023 – The Diagnostic Settings Storage Retention feature will no longer be available to configure new retention rules for log data. This includes using the portal, CLI PowerShell, and ARM and Bicep templates. If you have configured retention settings, you'll still be able to see and change them in the portal.

March 31, 2024 – You will no longer be able to use the API (CLI, Powershell, or templates), or Azure portal to configure retention setting unless you're changing them to 0. Existing retention rules will still be respected.

September 30, 2025 – All retention functionality for the Diagnostic Settings Storage Retention feature will be disabled across all environments.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.1.5 Ensure that Network Security Group Flow logs are captured and sent to Log Analytics (Manual)

Profile Applicability:

- Level 2

Description:

Ensure that network flow logs are captured and fed into a central log analytics workspace.

Rationale:

Network Flow Logs provide valuable insight into the flow of traffic around your network and feed into both Azure Monitor and Azure Sentinel (if in use), permitting the generation of visual flow diagrams to aid with analyzing for lateral movement, etc.

Impact:

The impact of configuring NSG Flow logs is primarily one of cost and configuration. If deployed, it will create storage accounts that hold minimal amounts of data on a 5-day lifecycle before feeding to Log Analytics Workspace. This will increase the amount of data stored and used by Azure Monitor.

Audit:

Audit from Azure Portal

1. Navigate to `Network Watcher`.
2. Under `Logs`, select `Flow logs`.
3. Click `Add filter`.
4. From the `Filter` drop-down, select `Flow log type`.
5. From the `Value` drop-down, check `Network security group` only.
6. Click `Apply`.
7. Ensure that at least one network security group flow log is listed and is configured to send logs to a `Log Analytics Workspace`.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 27960feb-a23c-4577-8d36-ef8b5f35e0be **- Name:** 'All flow log resources should be in enabled state'
- **Policy ID:** c251913d-7d24-4958-af87-478ed3b9ba41 **- Name:** 'Flow logs should be configured for every network security group'

- **Policy ID:** 4c3c6c5f-0d47-4402-99b8-aa543dd8bcee **- Name:** 'Flow logs should be configured for every virtual network'

Remediation:

Remediate from Azure Portal

1. Navigate to `Network Watcher`.
2. Under `Logs`, select `Flow logs`.
3. Select `+ Create`.
4. Select the desired Subscription.
5. For `Flow log type`, select `Network security group`.
6. Select `+ Select target resource`.
7. Select `Network security group`.
8. Select a network security group.
9. Click `Confirm selection`.
10. Select or create a new Storage Account.
11. If using a v2 storage account, input the retention in days to retain the log.
12. Click `Next`.
13. Under `Analytics`, for `Flow log version`, select `Version 2`.
14. Check the box next to `Enable traffic analytics`.
15. Select a processing interval.
16. Select a `Log Analytics Workspace`.
17. Select `Next`.
18. Optionally add Tags.
19. Select `Review + create`.
20. Select `Create`.

Warning
The remediation policy creates remediation deployment and names them by concatenating the subscription name and the resource group name. The MAXIMUM permitted length of a deployment name is 64 characters. Exceeding this will cause the remediation task to fail.

Default Value:

By default Network Security Group logs are not sent to Log Analytics.

References:

1. https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-4-enable-network-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.6 Collect Network Traffic Flow Logs Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		●	●
v7	12.8 Deploy NetFlow Collection on Networking Boundary Devices Enable the collection of NetFlow and logging data on all network boundary devices.		●	●

6.1.6 Ensure that logging for Azure AppService 'HTTP logs' is enabled (Manual)

Profile Applicability:

- Level 2

Description:

Enable AppServiceHTTPLogs diagnostic log category for Azure App Service instances to ensure all http requests are captured and centrally logged.

Rationale:

Capturing web requests can be important supporting information for security analysts performing monitoring and incident response activities. Once logging, these logs can be ingested into SIEM or other central aggregation point for the organization.

Impact:

Log consumption and processing will incur additional cost.

Audit:

Audit from Azure Portal

1. Go to `App Services`.

For each `App Service`:

2. Under `Monitoring`, go to `Diagnostic settings`.
3. Ensure a diagnostic setting exists that logs `HTTP logs` to a destination aligned to your environment's approach to log consumption (event hub, storage account, etc. dependent on what is consuming the logs such as SIEM or other log aggregation utility).

Remediation:

Remediate from Azure Portal

1. Go to `App Services`.

For each `App Service`:

2. Under `Monitoring`, go to `Diagnostic settings`.
3. To update an existing diagnostic setting, click `Edit setting` against the setting. To create a new diagnostic setting, click `Add diagnostic setting` and provide a name for the new setting.

4. Check the checkbox next to `HTTP logs`.
5. Configure a destination based on your specific logging consumption capability (for example Stream to an event hub and then consuming with SIEM integration for Event Hub logging).
6. Click `Save`.

Default Value:

Not configured.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.7 Collect URL Request Audit Logs Collect URL request audit logs on enterprise assets, where appropriate and supported.		●	●
v7	7.6 Log all URL requests Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.		●	●

6.2 Monitoring using Activity Log Alerts

The recommendations provided in this section are intended to provide entry-level alerting for crucial activities on a tenant account. These recommended activities **should** be tuned to your needs. By default, each of these Activity Log Alerts tends to guide the reader to alerting at the "Subscription-wide" level which will capture and alert on rules triggered by all resources and resource groups contained within a subscription. This is not an ideal rule set for Alerting within larger and more complex organizations.

While this section provides recommendations for the creation of **Activity Log Alerts** specifically, Microsoft Azure supports four different types of alerts:

- Metric Alerts
- Log Alerts
- Activity Log Alerts
- Smart Detection Alerts

All Azure services (Microsoft provided or otherwise) that can generate alerts are assigned a "Resource provider namespace" when they are registered in an Azure tenant. The recommendations in this section are in no way exhaustive of the plethora of available "Providers" or "Resource Types." The Resource Providers that are registered in your Azure Tenant can be located in your Subscription. Each registered Provider in your environment **may** have available "Conditions" to raise alerts via Activity Log Alerts. These providers should be considered for inclusion in Activity Log Alert rules of your own making.

To view the registered resource providers in your Subscription(s), use this guide:

- https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-providers-and-types

If you wish to create custom alerting rules for Activity Log Alerts or other alert types, please refer to Microsoft documentation:

- https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-create-new-alert-rule

6.2.1 Ensure that Activity Log Alert exists for Create Policy Assignment (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create Policy Assignment event.

Rationale:

Monitoring for create policy assignment events gives insight into changes done in "Azure policy - assignments" and can reduce the time it takes to detect unsolicited changes.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Authorization/policyAssignments/write`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Create policy assignment'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription ID> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Authorization/policyAssignments/write` in the output. If it's missing, generate a finding.

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Authorization/policyAssignments/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

If the output is empty, an `alert rule` for `Create Policy Assignments` is not configured.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** c5447c04-a4d7-4ba8-a263-c9ee321a6858 **- Name:** 'An activity log alert should exist for specific Policy operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Create policy assignment (Policy assignment)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Authorization/policyAssignments/write and
level=<verbose | information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription ID> --action-group <action group ID>
```

Remediate from PowerShell

Create the `conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Authorization/policyAssignments/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Get the `Action Group` information and store it in a variable, then create a new `Action` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` variable.

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Authorization/policyAssignments/write`

```
New-AzActivityLogAlert -Name "<activity alert rule name>" -ResourceGroupName
"<resource group name>" -Condition $conditions -Scope $scope -Location global
-Action $actionObject -Subscription <subscription ID> -Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
6. https://docs.microsoft.com/en-in/rest/api/policy/policy-assignments
7. https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-log

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.2.2 Ensure that Activity Log Alert exists for Delete Policy Assignment (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Delete Policy Assignment event.

Rationale:

Monitoring for delete policy assignment events gives insight into changes done in "azure policy - assignments" and can reduce the time it takes to detect unsolicited changes.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Authorization/policyAssignments/delete`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Delete policy assignment'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription ID> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Authorization/policyAssignments/delete` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Authorization/policyAssignments/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** c5447c04-a4d7-4ba8-a263-c9ee321a6858 **- Name:** 'An activity log alert should exist for specific Policy operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Delete policy assignment (Policy assignment)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Authorization/policyAssignments/delete and
level=<verbose | information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell

Create the conditions object

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Authorization/policyAssignments/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Action` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` variable.

```
$scope = "/subscriptions/<subscription id>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Authorization/policyAssignments/delete`.

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
2. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
5. https://azure.microsoft.com/en-us/services/blueprints/

Additional Information:

This log alert also applies for Azure Blueprints.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.2.3 Ensure that Activity Log Alert exists for Create or Update Network Security Group (Automated)

Profile Applicability:

- Level 1

Description:

Create an Activity Log Alert for the Create or Update Network Security Group event.

Rationale:

Monitoring for Create or Update Network Security Group events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Network/networkSecurityGroups/write`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Create or Update Network Security Group'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription ID> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Network/networkSecurityGroups/write` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Network/networkSecurityGroups/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Create or Update Network Security Group (Network Security Group)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Network/networkSecurityGroups/write and level=verbose
--scope "/subscriptions/<subscription ID>" --name "<activity log rule name>"
--subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Network/networkSecurityGroups/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription id>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Network/networkSecurityGroups/write`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.2.4 Ensure that Activity Log Alert exists for Delete Network Security Group (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Delete Network Security Group event.

Rationale:

Monitoring for "Delete Network Security Group" events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Network/networkSecurityGroups/delete`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Delete Network Security Group'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription ID> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Network/networkSecurityGroups/delete` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Network/networkSecurityGroups/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Delete Network Security Group (Network Security Group)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Network/networkSecurityGroups/delete and
level=<verbose | information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Network/networkSecurityGroups/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription id>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Network/networkSecurityGroups/delete`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.2.5 Ensure that Activity Log Alert exists for Create or Update Security Solution (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create or Update Security Solution event.

Rationale:

Monitoring for Create or Update Security Solution events gives insight into changes to the active security solutions and may reduce the time it takes to detect suspicious activity.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Security/securitySolutions/write`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Create or Update Security Solutions'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Security/securitySolutions/write` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Security/securitySolutions/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Create or Update Security Solutions (Security Solutions)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Security/securitySolutions/write and level=<verbose |
information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Security/securitySolutions/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Security/securitySolutions/write`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.2.6 Ensure that Activity Log Alert exists for Delete Security Solution (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Delete Security Solution event.

Rationale:

Monitoring for Delete Security Solution events gives insight into changes to the active security solutions and may reduce the time it takes to detect suspicious activity.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Security/securitySolutions/delete`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Delete Security Solutions'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Security/securitySolutions/delete` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Security/securitySolutions/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Delete Security Solutions (Security Solutions)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Security/securitySolutions/delete and level=<verbose
| information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Security/securitySolutions/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Security/securitySolutions/delete`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.2.7 Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create or Update SQL Server Firewall Rule event.

Rationale:

Monitoring for Create or Update SQL Server Firewall Rule events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Impact:

There will be a substantial increase in log size if there are a large number of administrative actions on a server.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Sql/servers/firewallRules/write`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Create/Update server firewall rule'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Sql/servers/firewallRules/write` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Sql/servers/firewallRules/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Create/Update server firewall rule (Server Firewall Rule)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Sql/servers/firewallRules/write and level=<verbose |
information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Sql/servers/firewallRules/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Sql/servers/firewallRules/write`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.2.8 Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the "Delete SQL Server Firewall Rule."

Rationale:

Monitoring for Delete SQL Server Firewall Rule events gives insight into SQL network access changes and may reduce the time it takes to detect suspicious activity.

Impact:

There will be a substantial increase in log size if there are a large number of administrative actions on a server.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Sql/servers/firewallRules/delete`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Delete server firewall rule'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Sql/servers/firewallRules/delete` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Sql/servers/firewallRules/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** b954148f-4c11-4c38-8221-be76711e194a **- Name:** 'An activity log alert should exist for specific Administrative operations'

Remediation:
Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Delete server firewall rule (Server Firewall Rule)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Sql/servers/firewallRules/delete and level=<verbose |
information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell
Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Sql/servers/firewallRules/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Sql/servers/firewallRules/delete`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.2.9 Ensure that Activity Log Alert exists for Create or Update Public IP Address rule (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create or Update Public IP Addresses rule.

Rationale:

Monitoring for Create or Update Public IP Address events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Impact:

There will be a substantial increase in log size if there are a large number of administrative actions on a server.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Network/publicIPAddresses/write`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Create or Update Public Ip Address'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Network/publicIPAddresses/write` in the output
Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Network/publicIPAddresses/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 1513498c-3091-461a-b321-e9b433218d28 **- Name:** 'Enable logging by category group for Public IP addresses (microsoft.network/publicipaddresses) to Log Analytics'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Create or Update Public Ip Address (Public Ip Address)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Network/publicIPAddresses/write and level=<verbose |
information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Network/publicIPAddresses/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the Action Group information and store in a variable, then create the Actions object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the Scope object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the Activity Log Alert Rule for Microsoft.Network/publicIPAddresses/write

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.2.10 Ensure that Activity Log Alert exists for Delete Public IP Address rule (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Delete Public IP Address rule.

Rationale:

Monitoring for Delete Public IP Address events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Impact:

There will be a substantial increase in log size if there are a large number of administrative actions on a server.

Audit:

Audit from Azure Portal

1. Navigate to the `Monitor` blade.
2. Click on `Alerts`.
3. In the Alerts window, click on `Alert rules`.
4. Ensure an alert rule exists where the Condition column contains `Operation name=Microsoft.Network/publicIPAddresses/delete`.
5. Click on the Alert `Name` associated with the previous step.
6. Ensure the `Condition` panel displays the text `Whenever the Activity Log has an event with Category='Administrative', Operation name='Delete Public Ip Address'` and does not filter on `Level`, `Status` or `Caller`.
7. Ensure the `Actions` panel displays an Action group is assigned to notify the appropriate personnel in your organization.

Audit from Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query
"[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Network/publicIPAddresses/delete` in the output

Audit from PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_.ConditionAllOf.Equal -match
"Microsoft.Network/publicIPAddresses/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 1513498c-3091-461a-b321-e9b433218d28 **- Name:** 'Enable logging by category group for Public IP addresses (microsoft.network/publicipaddresses) to Log Analytics'

Remediation:

Remediate from Azure Portal

1. Navigate to the `Monitor` blade.
2. Select `Alerts`.
3. Select `Create`.
4. Select `Alert rule`.
5. Choose a subscription.
6. Select `Apply`.
7. Select the `Condition` tab.
8. Click `See all signals`.
9. Select `Delete Public Ip Address (Public Ip Address)`.
10. Click `Apply`.
11. Select the `Actions` tab.
12. Click `Select action groups` to select an existing action group, or `Create action group` to create a new action group.
13. Follow the prompts to choose or create an action group.
14. Select the `Details` tab.
15. Select a `Resource group`, provide an `Alert rule name` and an optional `Alert rule description`.
16. Click `Review + create`.
17. Click `Create`.

Remediate from Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Network/publicIPAddresses/delete and level=<verbose |
information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID>
```

Remediate from PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Network/publicIPAddresses/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Network/publicIPAddresses/delete`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

Default Value:

By default, no monitoring alerts are created.

References:

1. https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement
2. https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log
3. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate
4. https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

6.3 Configuring Application Insights

6.3.1 Ensure Application Insights are Configured (Automated)

Profile Applicability:

- Level 2

Description:

Application Insights within Azure act as an Application Performance Monitoring solution providing valuable data into how well an application performs and additional information when performing incident response. The types of log data collected include application metrics, telemetry data, and application trace logging data providing organizations with detailed information about application activity and application transactions. Both data sets help organizations adopt a proactive and retroactive means to handle security and performance related metrics within their modern applications.

Rationale:

Configuring Application Insights provides additional data not found elsewhere within Azure as part of a much larger logging and monitoring program within an organization's Information Security practice. The types and contents of these logs will act as both a potential cost saving measure (application performance) and a means to potentially confirm the source of a potential incident (trace logging). Metrics and Telemetry data provide organizations with a proactive approach to cost savings by monitoring an application's performance, while the trace logging data provides necessary details in a reactive incident response scenario by helping organizations identify the potential source of an incident within their application.

Impact:

Because Application Insights relies on a Log Analytics Workspace, an organization will incur additional expenses when using this service.

Audit:

Audit from Azure Portal

1. Navigate to `Application Insights`.
2. Ensure an `Application Insights` service is configured and exists.

Audit from Azure CLI

```
az monitor app-insights component show --query "[].{ID:appId, Name:name,
Tenant:tenantId, Location:location, Provisioning_State:provisioningState}"
```

Ensure the above command produces output, otherwise `Application Insights` has not been configured.

Audit from PowerShell

```
Get-AzApplicationInsights|select
location,name,appid,provisioningState,tenantid
```

Remediation:

Remediate from Azure Portal

1. Navigate to `Application Insights`.
2. Under the `Basics` tab within the `PROJECT DETAILS` section, select the `Subscription`.
3. Select the `Resource group`.
4. Within the `INSTANCE DETAILS`, enter a `Name`.
5. Select a `Region`.
6. Next to `Resource Mode`, select `Workspace-based`.
7. Within the `WORKSPACE DETAILS`, select the `Subscription` for the log analytics workspace.
8. Select the appropriate `Log Analytics Workspace`.
9. Click `Next:Tags >`.
10. Enter the appropriate `Tags` as `Name`, `Value` pairs.
11. Click `Next:Review+Create`.
12. Click `Create`.

Remediate from Azure CLI

```
az monitor app-insights component create --app <app name> --resource-group
<resource group name> --location <location> --kind "web" --retention-time
<INT days to retain logs> --workspace <log analytics workspace ID> --
subscription <subscription ID>
```

Remediate from PowerShell

```
New-AzApplicationInsights -Kind "web" -ResourceGroupName <resource group
name> -Name <app insights name> -location <location> -RetentionInDays <INT
days to retain logs> -SubscriptionID <subscription ID> -WorkspaceResourceId
<log analytics workspace ID>
```

Default Value:

Application Insights are not enabled by default.

References:

1. https://learn.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.2 Collect Audit Logs Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	6.2 Activate audit logging Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

6.4 Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it (Manual)

Profile Applicability:

- Level 1

Description:

Resource Logs capture activity to the data access plane while the Activity log is a subscription-level log for the control plane. Resource-level diagnostic logs provide insight into operations that were performed within that resource itself; for example, reading or updating a secret from a Key Vault. Currently, 95 Azure resources support Azure Monitoring (See the more information section for a complete list), including Network Security Groups, Load Balancers, Key Vault, AD, Logic Apps, and CosmosDB. The content of these logs varies by resource type.

A number of back-end services were not configured to log and store Resource Logs for certain activities or for a sufficient length. It is crucial that monitoring is correctly configured to log all relevant activities and retain those logs for a sufficient length of time. Given that the mean time to detection in an enterprise is 240 days, a minimum retention period of two years is recommended.

Rationale:

A lack of monitoring reduces the visibility into the data plane, and therefore an organization's ability to detect reconnaissance, authorization attempts or other malicious activity. Unlike Activity Logs, Resource Logs are not enabled by default. Specifically, without monitoring it would be impossible to tell which entities had accessed a data store that was breached. In addition, alerts for failed attempts to access APIs for Web Services or Databases are only possible when logging is enabled.

Impact:

Costs for monitoring varies with Log Volume. Not every resource needs to have logging enabled. It is important to determine the security classification of the data being processed by the given resource and adjust the logging based on which events need to be tracked. This is typically determined by governance and compliance requirements.

Audit:

Audit from Azure Portal
The specific steps for configuring resources within the Azure console vary depending on resource, but typically the steps are:

1. Go to the resource
2. Click on Diagnostic settings
3. In the blade that appears, click "Add diagnostic setting"

4. Configure the diagnostic settings
5. Click on Save

Audit from Azure CLI
List all `resources` for a `subscription`

```
az resource list --subscription <subscription id>
```

For each `resource` run the following

```
az monitor diagnostic-settings list --resource <resource ID>
```

An empty result means a `diagnostic settings` is not configured for that resource. An error message means a `diagnostic settings` is not supported for that resource.

Audit from PowerShell
Get a list of `resources` in a `subscription` context and store in a variable

```
$resources = Get-AzResource
```

Loop through each `resource` to determine if a diagnostic setting is configured or not.

```
foreach ($resource in $resources) {$diagnosticSetting = Get-
AzDiagnosticSetting -ResourceId $resource.id -ErrorAction "SilentlyContinue";
if ([string]::IsNullOrEmpty($diagnosticSetting)) {$message = "Diagnostic
Settings not configured for resource: " + $resource.Name;Write-Output
$message}else{$diagnosticSetting}}
```

A result of `Diagnostic Settings not configured for resource: <resource name>` means a `diagnostic settings` is not configured for that resource. Otherwise, the output of the above command will show configured `Diagnostic Settings` for a resource.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** cf820ca0-f99e-4f3e-84fb-66e913812d21 **- Name:** 'Resource logs in Key Vault should be enabled'
- **Policy ID:** 91a78b24-f231-4a8a-8da9-02c35b2b6510 **- Name:** 'App Service apps should have resource logs enabled'
- **Policy ID:** 428256e6-1fac-4f48-a757-df34c2b3336d **- Name:** 'Resource logs in Batch accounts should be enabled'
- **Policy ID:** 057ef27e-665e-4328-8ea3-04b3122bd9fb **- Name:** 'Resource logs in Azure Data Lake Store should be enabled'
- **Policy ID:** c95c74d9-38fe-4f0d-af86-0c7d626a315c **- Name:** 'Resource logs in Data Lake Analytics should be enabled'
- **Policy ID:** 83a214f7-d01a-484b-91a9-ed54470c9a6a **- Name:** 'Resource logs in Event Hub should be enabled'

- **Policy ID:** 383856f8-de7f-44a2-81fc-e5135b5c2aa4 **- Name:** 'Resource logs in IoT Hub should be enabled'
- **Policy ID:** 34f95f76-5386-4de7-b824-0d8478470c9d **- Name:** 'Resource logs in Logic Apps should be enabled'
- **Policy ID:** b4330a05-a843-4bc8-bf9a-cacce50c67f4 **- Name:** 'Resource logs in Search services should be enabled'
- **Policy ID:** f8d36e2f-389b-4ee4-898d-21aeb69a0f45 **- Name:** 'Resource logs in Service Bus should be enabled'
- **Policy ID:** f9be5368-9bf5-4b84-9e0a-7850da98bb46 **- Name:** 'Resource logs in Azure Stream Analytics should be enabled'

Remediation:

Azure Subscriptions should log every access and operation for all resources.
Logs should be sent to Storage and a Log Analytics Workspace or equivalent third-party system. Logs should be kept in readily accessible storage for a minimum of one year, and then moved to inexpensive cold storage for a duration of time as necessary. If retention policies are set but storing logs in a Storage Account is disabled (for example, if only Event Hubs or Log Analytics options are selected), the retention policies have no effect. Enable all monitoring at first, and then be more aggressive moving data to cold storage if the volume of data becomes a cost concern.

Remediate from Azure Portal

The specific steps for configuring resources within the Azure console vary depending on resource, but typically the steps are:

1. Go to the resource
2. Click on Diagnostic settings
3. In the blade that appears, click "Add diagnostic setting"
4. Configure the diagnostic settings
5. Click on Save

Remediate from Azure CLI

For each `resource`, run the following making sure to use a `resource` appropriate JSON encoded `category` for the `--logs` option.

```
az monitor diagnostic-settings create --name <diagnostic settings name> --
resource <resource ID> --logs "[{category:<resource specific
category>,enabled:true,rentention-policy:{enabled:true,days:180}}]" --metrics
"[{category:AllMetrics,enabled:true,retention-
policy:{enabled:true,days:180}}]" <[--event-hub <event hub ID> --event-hub-
rule <event hub auth rule ID> | --storage-account <storage account ID> |--
workspace <log analytics workspace ID> | --marketplace-partner-id <full
resource ID of third-party solution>]>
```

Remediate from PowerShell

Create the `log` settings object

```
$logSettings = @()
$logSettings += New-AzDiagnosticSettingLogSettingsObject -Enabled $true -
RetentionPolicyDay 180 -RetentionPolicyEnabled $true -Category <resource
specific category>
$logSettings += New-AzDiagnosticSettingLogSettingsObject -Enabled $true -
RetentionPolicyDay 180 -RetentionPolicyEnabled $true -Category <resource
specific category number 2>
```

Create the `metric` settings object

```
$metricSettings = @()
$metricSettings += New-AzDiagnosticSettingMetricSettingsObject -Enabled $true
-RetentionPolicyDay 180 -RetentionPolicyEnabled $true -Category AllMetrics
```

Create the diagnostic setting for a specific resource

```
New-AzDiagnosticSetting -Name "<diagnostic settings name>" -ResourceId
<resource ID> -Log $logSettings -Metric $metricSettings
```

Default Value:

By default, Azure Monitor Resource Logs are 'Disabled' for all resources.

References:

1. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-3-enable-logging-for-security-investigation
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-5-centralize-security-log-management-and-analysis
3. https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/monitor-azure-resource
4. Supported Log Categories: https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/resource-logs-categories
5. Logs and Audit - Fundamentals: https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit
6. Collecting Logs: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-activity-logs
7. Key Vault Logging: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-logging
8. Monitor Diagnostic Settings: https://docs.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?view=azure-cli-latest
9. Overview of Diagnostic Logs: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-logs-overview
10. Supported Services for Diagnostic Logs: https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-logs-schema
11. Diagnostic Logs for CDNs: https://docs.microsoft.com/en-us/azure/cdn/cdn-azure-diagnostic-logs

Additional Information:

Note: The CIS Benchmark covers some specific Diagnostic Logs separately – e.g.

```
"Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and
'Delete' requests"

"Ensure that Network Security Group Flow Log retention period is 'greater
than 90 days'"
```

For an up-to-date list of Azure resources which support Azure Monitor, refer to the "Supported Log Categories" reference.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.5 Collect Detailed Audit Logs Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v8	8.9 Centralize Audit Logs Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	6.3 Enable Detailed Logging Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	6.5 Central Log Management Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

6.5 Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) (Manual)

Profile Applicability:

- Level 2

Description:

The use of Basic or Free SKUs in Azure whilst cost effective have significant limitations in terms of what can be monitored and what support can be realized from Microsoft. Typically, these SKU's do not have a service SLA and Microsoft may refuse to provide support for them. Consequently Basic/Free SKUs should never be used for production workloads.

Rationale:

Typically, production workloads need to be monitored and should have an SLA with Microsoft, using Basic SKUs for any deployed product will mean that that these capabilities do not exist.

The following resource types should use standard SKUs as a minimum.

- Public IP Addresses
- Network Load Balancers
- REDIS Cache
- SQL PaaS Databases
- VPN Gateways

Impact:

The impact of enforcing Standard SKU's is twofold

1. There will be a cost increase
2. The monitoring and service level agreements will be available and will support the production service.

All resources should be either tagged or in separate Management Groups/Subscriptions

Audit:

This needs to be audited by Azure Policy (one for each resource type) and denied for each artifact that is production.

Audit from Azure Portal

1. Open `Azure Resource Graph Explorer`
2. Click `New query`
3. Paste the following into the query window:

```
Resources
| where sku contains 'Basic' or sku contains 'consumption'
| order by type
```

4. Click `Run query` then evaluate the results in the results window.
5. Ensure that no production artifacts are returned.

Audit from Azure CLI

```
az graph query -q "Resources | where sku contains 'Basic' or sku contains
'consumption' | order by type"
```

Alternatively, to filter on a specific resource group:

```
az graph query -q "Resources | where resourceGroup == '<resourceGroupName>' |
where sku contains 'Basic' or sku contains 'consumption' | order by type"
```

Ensure that no production artifacts are returned.

Audit from PowerShell

```
Get-AzResource | ?{ $_.Sku -EQ "Basic"}
```

Ensure that no production artifacts are returned.

Remediation:

Each artifact has its own process for upgrading from basic to standard SKU's and this should be followed if required.

Default Value:

Policy should enforce standard SKUs for the following artifacts:

- Public IP Addresses
- Network Load Balancers
- REDIS Cache
- SQL PaaS Databases
- VPN Gateways

References:

1. https://azure.microsoft.com/en-us/support/plans
2. https://azure.microsoft.com/en-us/support/plans/response/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 Ensure Authorized Software is Currently Supported Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	●	●	●
v7	2.2 Ensure Software is Supported by Vendor Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	●	●	●

7 Networking

This section covers security recommendations to follow in order to set networking policies on an Azure subscription.

7.1 Ensure that RDP access from the Internet is evaluated and restricted (Automated)

Profile Applicability:

- Level 1

Description:

Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required.

Rationale:

The potential security problem with using RDP over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use a virtual machine as a launch point for compromising other machines on an Azure Virtual Network or even attack networked devices outside of Azure.

Audit:

Audit from Azure Portal

1. For each VM, open the `Networking` blade
2. Verify that the `INBOUND PORT RULES` **does not** have a rule for RDP such as
   - port = `3389`,
   - protocol = `TCP` OR `ANY`,
   - Source = `Any` OR `Internet`

Audit from Azure CLI

List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"
"destinationPortRange" : "3389" or "*" or "[port range containing 3389]"
"direction" : "Inbound"
"protocol" : "TCP" or "*"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or
"any"
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 22730e10-96f6-4aac-ad84-9383d35b5917 **- Name:** 'Management ports should be closed on your virtual machines'

Remediation:

Where RDP is not explicitly required and narrowly configured for resources attached to the Network Security Group, Internet-level access to your Azure resources should be restricted or eliminated.
For internal access to relevant resources, configure an encrypted network tunnel such as:
ExpressRoute
Site-to-site VPN
Point-to-site VPN

Default Value:

By default, RDP access from internet is not `enabled`.

References:

1. https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices#disable-rdpssh-access-to-azure-virtual-machines
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-1-establish-network-segmentation-boundaries
3. Express Route: https://docs.microsoft.com/en-us/azure/expressroute/
4. Site-to-Site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal
5. Point-to-Site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	13.4 Perform Traffic Filtering Between Network Segments Perform traffic filtering between network segments, where appropriate.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

7.2 Ensure that SSH access from the Internet is evaluated and restricted (Automated)

Profile Applicability:

- Level 1

Description:

Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required.

Rationale:

The potential security problem with using SSH over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use a virtual machine as a launch point for compromising other machines on the Azure Virtual Network or even attack networked devices outside of Azure.

Audit:

Audit from Azure Portal

1. Open the `Networking` blade for the specific Virtual machine in Azure portal
2. Verify that the `INBOUND PORT RULES` **does not** have a rule for SSH such as
   - port = `22`,
   - protocol = `TCP` OR `ANY`,
   - Source = `Any` OR `Internet`

Audit from Azure CLI

List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"
"destinationPortRange" : "22" or "*" or "[port range containing 22]"
"direction" : "Inbound"
"protocol" : "TCP" or "*"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or
"any"
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 22730e10-96f6-4aac-ad84-9383d35b5917 **- Name:** 'Management ports should be closed on your virtual machines'

Remediation:

Where SSH is not explicitly required and narrowly configured for resources attached to the Network Security Group, Internet-level access to your Azure resources should be restricted or eliminated.
For internal access to relevant resources, configure an encrypted network tunnel such as:
ExpressRoute
Site-to-site VPN
Point-to-site VPN

Default Value:

By default, SSH access from internet is not `enabled`.

References:

1. https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices#disable-rdpssh-access-to-azure-virtual-machines
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-1-establish-network-segmentation-boundaries
3. Express Route: https://docs.microsoft.com/en-us/azure/expressroute/
4. Site-to-Site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal
5. Point-to-Site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	13.4 Perform Traffic Filtering Between Network Segments Perform traffic filtering between network segments, where appropriate.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

7.3 Ensure that UDP access from the Internet is evaluated and restricted (Automated)

Profile Applicability:

- Level 1

Description:

Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required.

Rationale:

The potential security problem with broadly exposing UDP services over the Internet is that attackers can use DDoS amplification techniques to reflect spoofed UDP traffic from Azure Virtual Machines. The most common types of these attacks use exposed DNS, NTP, SSDP, SNMP, CLDAP and other UDP-based services as amplification sources for disrupting services of other machines on the Azure Virtual Network or even attack networked devices outside of Azure.

Audit:

Audit from Azure Portal

1. Open the `Networking` blade for the specific Virtual machine in Azure portal
2. Verify that the `INBOUND PORT RULES` **does not** have a rule for UDP such as

- protocol = `UDP`,
- Source = `Any` OR `Internet`

Audit from Azure CLI

List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"
"destinationPortRange" : "*" or "[port range containing 53, 123, 161, 389,
1900, or other vulnerable UDP-based services]"
"direction" : "Inbound"
"protocol" : "UDP"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or
"any"
```

Remediation:

Where UDP is not explicitly required and narrowly configured for resources attached to the Network Security Group, Internet-level access to your Azure resources should be restricted or eliminated.
For internal access to relevant resources, configure an encrypted network tunnel such as:
ExpressRoute
Site-to-site VPN
Point-to-site VPN

Default Value:

By default, UDP access from internet is not `enabled`.

References:

1. https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices#secure-your-critical-azure-service-resources-to-only-your-virtual-networks
2. https://docs.microsoft.com/en-us/azure/security/fundamentals/ddos-best-practices
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-1-establish-network-segmentation-boundaries
4. ExpressRoute: https://docs.microsoft.com/en-us/azure/expressroute/
5. Site-to-site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal
6. Point-to-site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	13.4 Perform Traffic Filtering Between Network Segments Perform traffic filtering between network segments, where appropriate.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

7.4 Ensure that HTTP(S) access from the Internet is evaluated and restricted (Automated)

Profile Applicability:

- Level 1

Description:

Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required and narrowly configured.

Rationale:

The potential security problem with using HTTP(S) over the Internet is that attackers can use various brute force techniques to gain access to Azure resources. Once the attackers gain access, they can use the resource as a launch point for compromising other resources within the Azure tenant.

Audit:

Audit from Azure Portal

1. For each VM, open the Networking blade
2. Verify that the INBOUND PORT RULES does not have a rule for HTTP(S) such as
    - port = `80`/ `443`,
    - protocol = `TCP`,
    - Source = `Any` OR `Internet`

Audit from Azure CLI

List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"
"destinationPortRange" : "80/443" or "*" or "[port range containing 80/443]"
"direction" : "Inbound"
"protocol" : "TCP"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or
"any"
```

Remediation:

Remediate from Azure Portal

1. Go to `Virtual machines`.
2. For each VM, open the `Networking` blade.
3. Click on `Inbound port rules`.
4. Delete the rule with:
    - Port = 80/443 OR [port range containing 80/443]
    - Protocol = TCP OR Any
    - Source = Any (*) OR IP Addresses(0.0.0.0/0) OR Service Tag(Internet)
    - Action = Allow

Remediate from Azure CLI

1. Run below command to list network security groups:

```
az network nsg list --subscription <subscription-id> --output table
```

2. For each network security group, run below command to list the rules associated with the specified port:

```
az network nsg rule list --resource-group <resource-group> --nsg-name
<nsg-name> --query "[?destinationPortRange=='80 or 443']"
```

3. Run the below command to delete the rule with:
    - Port = 80/443 OR [port range containing 80/443]
    - Protocol = TCP OR "*"
    - Source = Any (*) OR IP Addresses(0.0.0.0/0) OR Service Tag(Internet)
    - Action = Allow

```
az network nsg rule delete --resource-group <resource-group> --nsg-name
<nsg-name> --name <rule-name>
```

References:

1. Express Route: https://docs.microsoft.com/en-us/azure/expressroute/
2. Site-to-Site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal
3. Point-to-Site VPN: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-1-establish-network-segmentation-boundaries

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.4 Implement and Manage a Firewall on Servers Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	4.5 Implement and Manage a Firewall on End-User Devices Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	13.4 Perform Traffic Filtering Between Network Segments Perform traffic filtering between network segments, where appropriate.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

7.5 Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' (Automated)

Profile Applicability:

- Level 2

Description:

Network Security Group Flow Logs should be enabled and the retention period set to greater than or equal to 90 days.

Rationale:

Flow logs enable capturing information about IP traffic flowing in and out of network security groups. Logs can be used to check for anomalies and give insight into suspected breaches.

Impact:

This will keep IP traffic logs for longer than 90 days. As a level 2, first determine your need to retain data, then apply your selection here. As this is data stored for longer, your monthly storage costs will increase depending on your data use.

Audit:

Audit from Azure Portal

1. Go to `Network Watcher`
2. Select `NSG flow logs` blade in the Logs section
3. Select each Network Security Group from the list
4. Ensure `Status` is set to `On`
5. Ensure `Retention (days)` setting `greater than 90 days`

Audit from Azure CLI

```
az network watcher flow-log show --resource-group <resourceGroup> --nsg
<NameorID of the NetworkSecurityGroup> --query 'retentionPolicy'
```

Ensure that `enabled` is set to `true` and `days` is set to `greater then or equal to 90`.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 5e1cd26a-5090-4fdb-9d6a-84a90335e22d **- Name:** 'Configure network security groups to use specific workspace, storage account and flowlog retention policy for traffic analytics'

Remediation:

Remediate from Azure Portal

1. Go to `Network Watcher`
2. Select `NSG flow logs` blade in the Logs section
3. Select each Network Security Group from the list
4. Ensure `Status` is set to `On`
5. Ensure `Retention (days)` setting `greater than 90 days`
6. Select your storage account in the `Storage account` field
7. Select `Save`

Remediate from Azure CLI

Enable the `NSG flow logs` and set the Retention (days) to greater than or equal to 90 days.

```
az network watcher flow-log configure --nsg <NameorID of the Network Security
Group> --enabled true --resource-group <resourceGroupName> --retention 91 --
storage-account <NameorID of the storage account to save flow logs>
```

Default Value:

By default, Network Security Group Flow Logs are `disabled`.

References:

1. https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview
2. https://docs.microsoft.com/en-us/cli/azure/network/watcher/flow-log?view=azure-cli-latest
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-6-configure-log-storage-retention

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	8.3 Ensure Adequate Audit Log Storage Ensure that logging destinations maintain adequate storage to comply with the enterprise’s audit log management process.	●	●	●
v8	8.10 Retain Audit Logs Retain audit logs across enterprise assets for a minimum of 90 days.		●	●
v7	6.4 Ensure adequate storage for logs Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

7.6 Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use (Automated)

Profile Applicability:

- Level 2

Description:

Enable Network Watcher for physical regions in Azure subscriptions.

Rationale:

Network diagnostic and visualization tools available with Network Watcher help users understand, diagnose, and gain insights to the network in Azure.

Impact:

There are additional costs per transaction to run and store network data. For high-volume networks these charges will add up quickly.

Audit:

Audit from Azure Portal

1. Use the Search bar to search for and click on the `Network Watcher` service.
2. From the Overview menu item, review each Network Watcher listed, and ensure that a network watcher is listed for each region in use by the subscription.

Audit from Azure CLI

```
az network watcher list --query
"[].{Location:location,State:provisioningState}" -o table
```

This will list all network watchers and their provisioning state.
Ensure `provisioningState` is `Succeeded` for each network watcher.

```
az account list-locations --query
"[?metadata.regionType=='Physical'].{Name:name,DisplayName:regionalDisplayNam
e}" -o table
```

This will list all physical regions that exist in the subscription.
Compare this list to the previous one to ensure that for each region in use, a network watcher exists with `provisioningState` set to `Succeeded`.

Audit from PowerShell

Get a list of Network Watchers

```
Get-AzNetworkWatcher
```

Make sure each watcher is set with the `ProvisioningState` setting set to `Succeeded` and all `Locations` that are in use by the subscription are using a watcher.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** b6e2945c-0b7b-40f5-9233-7a5323b5cdc6 **- Name:** 'Network Watcher should be enabled'

Remediation:

Opting out of Network Watcher automatic enablement is a permanent change. Once you opt-out you cannot opt-in without contacting support.
To manually enable Network Watcher in each region where you want to use Network Watcher capabilities, follow the steps below.
Remediate from Azure Portal

1. Use the Search bar to search for and click on the `Network Watcher` service.
2. Click `Create`.
3. Select a `Region` from the drop-down menu.
4. Click `Add`.

Remediate from Azure CLI

```
az network watcher configure --locations <region> --enabled true --resource-group <resource_group>
```

Default Value:

Network Watcher is automatically enabled. When you create or update a virtual network in your subscription, Network Watcher will be enabled automatically in your Virtual Network's region. There is no impact to your resources or associated charge for automatically enabling Network Watcher.

References:

1. https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview
2. https://learn.microsoft.com/en-us/cli/azure/network/watcher?view=azure-cli-latest
3. https://learn.microsoft.com/en-us/cli/azure/network/watcher?view=azure-cli-latest#az-network-watcher-configure
4. https://learn.microsoft.com/en-us/azure/network-watcher/network-watcher-create
5. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-logging-threat-detection#lt-4-enable-network-logging-for-security-investigation
6. https://azure.microsoft.com/en-ca/pricing/details/network-watcher/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.2 Establish and Maintain a Secure Network Architecture Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v8	12.4 Establish and Maintain Architecture Diagram(s) Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●
v7	12.1 Maintain an Inventory of Network Boundaries Maintain an up-to-date inventory of all of the organization's network boundaries.	●	●	●

7.7 Ensure that Public IP addresses are Evaluated on a Periodic Basis (Manual)

Profile Applicability:

- Level 1

Description:

Public IP Addresses provide tenant accounts with Internet connectivity for resources contained within the tenant. During the creation of certain resources in Azure, a Public IP Address may be created. All Public IP Addresses within the tenant should be periodically reviewed for accuracy and necessity.

Rationale:

Public IP Addresses allocated to the tenant should be periodically reviewed for necessity. Public IP Addresses that are not intentionally assigned and controlled present a publicly facing vector for threat actors and significant risk to the tenant.

Audit:

Audit from Azure Portal

1. Open the `All Resources` blade
2. Click on `Add Filter`
3. In the Add Filter window, select the following:
   Filter: `Type`
   Operator: `Equals`
   Value: `Public IP address`
4. Click the `Apply` button
5. For each Public IP address in the list, use Overview (or Properties) to review the `"Associated to:"` field and determine if the associated resource is still relevant to your tenant environment. If the associated resource is relevant, ensure that additional controls exist to mitigate risk (e.g. Firewalls, VPNs, Traffic Filtering, Virtual Gateway Appliances, Web Application Firewalls, etc.) on all subsequently attached resources.

Audit from Azure CLI
List all Public IP addresses:

```
az network public-ip list
```

For each Public IP address in the output, review the `"name"` property and determine if the associated resource is still relevant to your tenant environment. If the associated resource is relevant, ensure that additional controls exist to mitigate risk (e.g. Firewalls, VPNs, Traffic Filtering, Virtual Gateway Appliances, Web Application Firewalls, etc.) on all subsequently attached resources.

Remediation:

Remediation will vary significantly depending on your organization's security requirements for the resources attached to each individual Public IP address.

Default Value:

During Virtual Machine and Application creation, a setting may create and attach a public IP.

References:

1. https://docs.microsoft.com/en-us/cli/azure/network/public-ip?view=azure-cli-latest
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.1 Ensure Network Infrastructure is Up-to-Date Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	●	●	●
v7	12.1 Maintain an Inventory of Network Boundaries Maintain an up-to-date inventory of all of the organization's network boundaries.	●	●	●

8 Virtual Machines

This section covers security recommendations to follow for the configuration of Virtual Machines on an Azure subscription.

8.1 Ensure an Azure Bastion Host Exists (Automated)

Profile Applicability:

- Level 2

Description:

The Azure Bastion service allows secure remote access to Azure Virtual Machines over the Internet without exposing remote access protocol ports and services directly to the Internet. The Azure Bastion service provides this access using TLS over 443/TCP, and subscribes to hardened configurations within an organization's Azure Active Directory service.

Rationale:

The Azure Bastion service allows organizations a more secure means of accessing Azure Virtual Machines over the Internet without assigning public IP addresses to those Virtual Machines. The Azure Bastion service provides Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to Virtual Machines using TLS within a web browser, thus preventing organizations from opening up 3389/TCP and 22/TCP to the Internet on Azure Virtual Machines. Additional benefits of the Bastion service includes Multi-Factor Authentication, Conditional Access Policies, and any other hardening measures configured within Azure Active Directory using a central point of access.

Impact:

The Azure Bastion service incurs additional costs and requires a specific virtual network configuration. The `Standard` tier offers additional configuration options compared to the `Basic` tier and may incur additional costs for those added features.

Audit:

Audit from Azure Portal

1. Click on `Bastions`
2. Ensure there is at least one `Bastion` host listed under the `Name` column

Audit from Azure CLI
Note: The Azure CLI `network bastion` module is in `Preview` as of this writing

```
az network bastion list --subscription <subscription ID>
```

Ensure the output of the above command is not empty.
Audit from PowerShell
Retrieve the `Bastion` host(s) information for a specific `Resource Group`

```
Get-AzBastion -ResourceGroupName <resource group name>
```

Ensure the output of the above command is not empty.

Remediation:

Remediate from Azure Portal

1. Click on Bastions
2. Select the Subscription
3. Select the Resource group
4. Type a Name for the new Bastion host
5. Select a Region
6. Choose Standard next to Tier
7. Use the slider to set the Instance count
8. Select the Virtual network or Create new
9. Select the Subnet named AzureBastionSubnet. Create a Subnet named AzureBastionSubnet using a /26 CIDR range if it doesn't already exist.
10. Selct the appropriate Public IP address option.
11. If Create new is selected for the Public IP address option, provide a Public IP address name.
12. If Use existing is selected for Public IP address option, select an IP address from Choose public IP address
13. Click Next: Tags >
14. Configure the appropriate Tags
15. Click Next: Advanced >
16. Select the appropriate Advanced options
17. Click Next: Review + create >
18. Click Create

Remediate from Azure CLI

```
az network bastion create --location <location> --name <name of bastion host>
--public-ip-address <public IP address name or ID> --resource-group <resource
group name or ID> --vnet-name <virtual network containing subnet called
"AzureBastionSubnet"> --scale-units <integer> --sku Standard [--disable-copy-
paste true|false] [--enable-ip-connect true|false] [--enable-tunneling
true|false]
```

Remediate from PowerShell

Create the appropriate Virtual network settings and Public IP Address settings.

```
$subnetName = "AzureBastionSubnet"
$subnet = New-AzVirtualNetworkSubnetConfig -Name $subnetName -AddressPrefix
<IP address range in CIDR notation making sure to use a /26>
$virtualNet = New-AzVirtualNetwork -Name <virtual network name> -
ResourceGroupName <resource group name> -Location <location> -AddressPrefix
<IP address range in CIDR notation> -Subnet $subnet
$publicip = New-AzPublicIpAddress -ResourceGroupName <resource group name> -
Name <public IP address name> -Location <location> -AllocationMethod Dynamic
-Sku Standard
```

Create the Azure Bastion service using the information within the created variables from above.

```
New-AzBastion -ResourceGroupName <resource group name> -Name <bastion name> -
PublicIpAddress $publicip -VirtualNetwork $virtualNet -Sku "Standard" -
ScaleUnit <integer>
```

Default Value:

By default, the Azure Bastion service is not configured.

References:

1. https://learn.microsoft.com/en-us/azure/bastion/bastion-overview#sku
2. https://learn.microsoft.com/en-us/powershell/module/az.network/get-azbastion?view=azps-9.2.0
3. https://learn.microsoft.com/en-us/cli/azure/network/bastion?view=azure-cli-latest

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.1 Ensure Network Infrastructure is Up-to-Date Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	●	●	●
v8	13.4 Perform Traffic Filtering Between Network Segments Perform traffic filtering between network segments, where appropriate.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●
v7	11.2 Document Traffic Configuration Rules All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual’s name responsible for that business need, and an expected duration of the need.		●	●
v7	12.1 Maintain an Inventory of Network Boundaries Maintain an up-to-date inventory of all of the organization's network boundaries.	●	●	●

8.2 Ensure Virtual Machines are utilizing Managed Disks (Automated)

Profile Applicability:

- Level 1

Description:

Migrate blob-based VHDs to Managed Disks on Virtual Machines to exploit the default features of this configuration. The features include:

1. Default Disk Encryption
2. Resilience, as Microsoft will managed the disk storage and move around if underlying hardware goes faulty
3. Reduction of costs over storage accounts

Rationale:

Managed disks are by default encrypted on the underlying hardware, so no additional encryption is required for basic protection. It is available if additional encryption is required. Managed disks are by design more resilient that storage accounts.

For ARM-deployed Virtual Machines, Azure Adviser will at some point recommend moving VHDs to managed disks both from a security and cost management perspective.

Impact:

There are additional costs for managed disks based off of disk space allocated. When converting to managed disks, VMs will be powered off and back on.

Audit:

Audit from Azure Portal

1. Using the search feature, go to `Virtual Machines`
2. Click the `Manage view` dropdown, then select `Edit columns`
3. Add `Uses managed disks` to the selected columns
4. Select `Save`
5. Ensure all virtual machines listed are using managed disks

Audit from PowerShell

```
Get-AzVM | ForEach-Object {"Name: " + $_.Name;"ManagedDisk Id: " +
$_.StorageProfile.OsDisk.ManagedDisk.Id;""}
```

Example output:

```
Name: vm1
ManagedDisk Id: /disk1/id

Name: vm2
ManagedDisk Id: /disk2/id
```

If the 'ManagedDisk Id' field is empty the os disk for that vm is not managed.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 06a78e20-9358-41c9-923c-fb736d382a4d **- Name:** 'Audit VMs that do not use managed disks'

Remediation:

Remediate from Azure Portal

1. Using the search feature, go to `Virtual Machines`
2. Select the virtual machine you would like to convert
3. Select `Disks` in the menu for the VM
4. At the top select `Migrate to managed disks`
5. You may follow the prompts to convert the disk and finish by selecting `Migrate` to start the process

NOTE VMs will be stopped and restarted after migration is complete.

Remediate from PowerShell

```
Stop-AzVM -ResourceGroupName $rgName -Name $vmName -Force
ConvertTo-AzVMManagedDisk -ResourceGroupName $rgName -VMName $vmName
Start-AzVM -ResourceGroupName $rgName -Name $vmName
```

Default Value:

Managed disks or are an option upon the creation of VMs.

References:

1. https://docs.microsoft.com/en-us/azure/virtual-machines/windows/convert-unmanaged-to-managed-disks

2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-4-enable-data-at-rest-encryption-by-default
3. https://docs.microsoft.com/en-us/azure/virtual-machines/faq-for-disks
4. https://azure.microsoft.com/en-us/pricing/details/managed-disks/

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

8.3 Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK) (Automated)

Profile Applicability:

- Level 2

Description:

Ensure that OS disks (boot volumes) and data disks (non-boot volumes) are encrypted with CMK (Customer Managed Keys). Customer Managed keys can be either ADE or Server Side Encryption (SSE).

Rationale:

Encrypting the IaaS VM's OS disk (boot volume) and Data disks (non-boot volume) ensures that the entire content is fully unrecoverable without a key, thus protecting the volume from unwanted reads. PMK (Platform Managed Keys) are enabled by default in Azure-managed disks and allow encryption at rest. CMK is recommended because it gives the customer the option to control which specific keys are used for the encryption and decryption of the disk. The customer can then change keys and increase security by disabling them instead of relying on the PMK key that remains unchanging. There is also the option to increase security further by using automatically rotating keys so that access to disk is ensured to be limited. Organizations should evaluate what their security requirements are, however, for the data stored on the disk. For high-risk data using CMK is a must, as it provides extra steps of security. If the data is low risk, PMK is enabled by default and provides sufficient data security.

Impact:

Using CMK/BYOK will entail additional management of keys.

NOTE: You must have your key vault set up to utilize this.

Audit:

Audit from Azure Portal

1. Go to `Virtual machines`.
2. For each virtual machine, go to `Settings`.
3. Click on `Disks`.
4. Ensure that the `OS disk` and `Data disks` have encryption set to CMK.

Audit from PowerShell

```
$ResourceGroupName="yourResourceGroupName"
$DiskName="yourDiskName"

$disk=Get-AzDisk -ResourceGroupName $ResourceGroupName -DiskName $DiskName
$disk.Encryption.Type
```

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 0961003e-5a0a-4549-abde-af6a37f2724d **- Name:** 'Virtual machines should encrypt temp disks, caches, and data flows between Compute and Storage resources'

Remediation:

Remediate from Azure Portal

Note: Disks must be detached from VMs to have encryption changed.

1. Go to `Virtual machines`
2. For each virtual machine, go to `Settings`
3. Click on `Disks`
4. Click the ellipsis (`...`), then click `Detach` to detach the disk from the VM
5. Now search for `Disks` and locate the unattached disk
6. Click the disk then select `Encryption`
7. Change your encryption type, then select your encryption set
8. Click `Save`
9. Go back to the VM and re-attach the disk

Remediate from PowerShell

```
$KVRGname = 'MyKeyVaultResourceGroup';
 $VMRGName = 'MyVirtualMachineResourceGroup';
 $vmName = 'MySecureVM';
 $KeyVaultName = 'MySecureVault';
 $KeyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName
$KVRGname;
 $diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;
 $KeyVaultResourceId = $KeyVault.ResourceId;

 Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGname -VMName $vmName
-DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -
DiskEncryptionKeyVaultId $KeyVaultResourceId;
```

NOTE:
During encryption it is likely that a reboot will be required. It may take up to 15 minutes to complete the process.
For Linux machines you may need to set the `-skipVmBackup` parameter.

Default Value:

By default, Azure disks are encrypted using SSE with PMK.

References:

1. https://docs.microsoft.com/azure/security/fundamentals/azure-disk-encryption-vms-vmss
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-disk-encryption?toc=%2fazure%2fsecurity%2ftoc.json
3. https://docs.microsoft.com/azure/security/fundamentals/data-encryption-best-practices#protect-data-at-resthttps://docs.microsoft.com/azure/virtual-machines/windows/disk-encryption-portal-quickstart
4. https://docs.microsoft.com/en-us/rest/api/compute/disks/delete
5. https://docs.microsoft.com/en-us/rest/api/compute/disks/update#encryptionsettings
6. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required
7. https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-enable-customer-managed-keys-powershell
8. https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

8.4 Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK) (Automated)

Profile Applicability:

- Level 2

Description:

Ensure that unattached disks in a subscription are encrypted with a Customer Managed Key (CMK).

Rationale:

Managed disks are encrypted by default with Platform-managed keys. Using Customer-managed keys may provide an additional level of security or meet an organization's regulatory requirements. Encrypting managed disks ensures that its entire content is fully unrecoverable without a key and thus protects the volume from unwarranted reads. Even if the disk is not attached to any of the VMs, there is always a risk where a compromised user account with administrative access to VM service can mount/attach these data disks, which may lead to sensitive information disclosure and tampering.

Impact:

NOTE: You must have your key vault set up to utilize this. Encryption is available only on Standard tier VMs. This might cost you more.

Utilizing and maintaining Customer-managed keys will require additional work to create, protect, and rotate keys.

Audit:

Audit from Azure Portal

1. Go to `Disks`
2. Click on `Add Filter`
3. In the `filter` field select `Disk state`
4. In the `Value` field select `Unattached`
5. Click `Apply`
6. for each disk listed ensure that `Encryption type` in the `encryption` blade is \`Encryption at-rest with a customer-managed key'

Audit from Azure CLI
Ensure command below does not return any output.

```
az disk list --query '[? diskstate == `Unattached`].{encryptionSettings:
encryptionSettings, name: name}' -o json
```

Sample Output:

```
[
 {
    "encryptionSettings": null,
    "name": "<Disk1>"
  },
  {
    "encryptionSettings": null,
    "name": "<Disk2>"
  }
]
```

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** ca91455f-eace-4f96-be59-e6e2c35b4816 **- Name:** 'Managed disks should be double encrypted with both platform-managed and customer-managed keys'

Remediation:

If data stored in the disk is no longer useful, refer to Azure documentation to delete unattached data disks at:

```
-https://docs.microsoft.com/en-us/rest/api/compute/disks/delete
-https://docs.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest#az-
disk-delete
```

If data stored in the disk is important, to encrypt the disk refer to azure documentation at:

```
-https://docs.microsoft.com/en-us/azure/virtual-machines/disks-enable-
customer-managed-keys-portal
-https://docs.microsoft.com/en-
us/rest/api/compute/disks/update#encryptionsettings
```

Default Value:

By default, managed disks are encrypted with a Platform-managed key.

References:

1. https://docs.microsoft.com/en-us/azure/security/fundamentals/azure-disk-encryption-vms-vmss
2. https://docs.microsoft.com/en-us/azure/security-center/security-center-disk-encryption?toc=%2fazure%2fsecurity%2ftoc.json
3. https://docs.microsoft.com/en-us/rest/api/compute/disks/delete
4. https://docs.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest#az-disk-delete

5. https://docs.microsoft.com/en-us/rest/api/compute/disks/update#encryptionsettings
6. https://docs.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest#az-disk-update
7. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

8.5 Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks' (Automated)

Profile Applicability:

- Level 1

Description:

Virtual Machine Disks and snapshots can be configured to allow access from different network resources.

Rationale:

The setting 'Enable public access from all networks' is, in many cases, an overly permissive setting on Virtual Machine Disks that presents atypical attack, data infiltration, and data exfiltration vectors. If a disk to network connection is required, the preferred setting is to 'Disable public access and enable private access.'

Impact:

The setting 'Disable public access and enable private access' will require configuring a private link (URL in references below).

The setting 'Disable public and private access' is most secure and preferred where disk network access is not needed.

Audit:

Audit from Azure Portal
Part A. Select the Virtual Machine to Evaluate

1. Using the search bar, search for and open the `Virtual Machines` service.
2. Click on the name of the Virtual Machine to be audited.

Part B. Evaluate each Virtual Machine Disk individually

1. From the selected Virtual Machine resource window, expand the `Settings` menu item and click `Disks.`
2. For each disk, click the name of the disk to open the disk resource window.
3. From the selected Disk resource window, expand the `Settings` menu item, and click `Networking`.

Ensure that Network access is **NOT** set to `Enable public access from all networks`.
Repeat Part B for each Disk attached to a VM.
Repeat Parts A and B to evaluate all Disks in all VMs.

Audit from PowerShell
For each managed disk, run the following PowerShell command:

```
Get-AzDisk -ResourceGroupName ‘<resource group name>’ -DiskName ‘<disk name>’
```

Ensure the `PublicNetworkAccess` setting is `Disabled` and the `NetworkAccessPolicy` is set to `AllowPrivate` or `DenyAll`.

Audit from Azure CLI
For each managed disk, run the following command:

```
az disk show --disk-name ‘<disk name>’ --resource-group ‘<resource group
name>’
```

Ensure the `publicNetworkAccess` setting is set to `Disabled` and the `networkAccessPolicy` setting is set to `AllowPrivate` or `DenyAll`.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- Policy ID: 8405fdab-1faf-48aa-b702-999c9c172094 - Name: 'Managed disks should disable public network access'

Remediation:

Remediate from Azure Portal
Part A. Select the Virtual Machine to Remediate

1. Using the search bar, search for and open the `Virtual Machines` service.
2. Click on the name of the Virtual Machine to be remediated.

Part B. Remediate each Virtual Machine Disk individually

1. From the selected Virtual Machine resource window, expand the `Settings` menu item and click `Disks.`
2. For each disk, click the name of the disk to open the disk resource window.
3. From the selected Disk resource window, expand the `Settings` menu item, and click `Networking`.

Under Network access, select the radio button for either:

- Disable public access and enable private access
- Disable public and private access

Repeat Part B for each Disk attached to a VM.
Repeat Parts A and B to remediate all Disks in all VMs.

Remediate from PowerShell

To disable `PublicNetworkAccess` and to set a `DenyAll` setting for the disk's `NetworkAccessPolicy` for each managed disk, run the following command:

```
$disk = Get-AzDisk -ResourceGroupName ‘<resource group name>’ -DiskName
‘<disk name>’
$disk.NetworkAccessPolicy = 'DenyAll'
$disk.PublicNetworkAccess = 'Disabled'
Update-AzDisk -ResourceGroup '<resource group name> -DiskName $disk.Name -
Disk $disk
```

To disable `PublicNetworkAccess` and to set an `AllowPrivate` setting for the disk's `NetworkAccessPolicy` for each managed disk, run the following command:

```
$disk = Get-AzDisk -ResourceGroupName ‘<resource group name>’ -DiskName
‘<disk name>’
$disk.NetworkAccessPolicy = 'AllowPrivate'
$disk.PublicNetworkAccess = 'Disabled'
$disk.DiskAccessId = '/subscriptions/<subscription
ID>/resourceGroups/<resource group
name>/providers/Microsoft.Compute/diskAccesses/<private disk access name>
Update-AzDisk -ResourceGroup '<resource group name> -DiskName $disk.Name -
Disk $disk
```

Remediate from Azure CLI

To configure a disk to allow private access only, run the following command making sure you have the `Disk Access ID` from a private disk access end point.

```
az disk update --name <managed disk name> --resource-group <resource group
name> --network-access-policy AllowPrivate --disk-access <disk access ID>
```

To completely disable public and private access for a disk, run the following command (still in preview) for each disk:

```
az disk update --name <managed disk name> --resource-group <resource group
name> --public-network-access Disabled --network-access-policy DenyAll
```

Default Value:

By default, Disk Network access is set to `Enable public access from all networks`.

References:

1. https://learn.microsoft.com/en-us/azure/virtual-machines/disks-enable-private-links-for-import-export-portal
2. https://learn.microsoft.com/en-us/azure/virtual-machines/linux/disks-export-import-private-links-cli

3. https://learn.microsoft.com/en-us/azure/virtual-machines/disks-restrict-import-export-overview

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

8.6 Ensure that 'Enable Data Access Authentication Mode' is 'Checked' (Automated)

Profile Applicability:

- Level 1

Description:

Data Access Authentication Mode provides a method of uploading or exporting Virtual Machine Disks.

Rationale:

Enabling `data access authentication mode` adds a layer of protection using an Entra ID role to further restrict users from creating and using Secure Access Signature (SAS) tokens for exporting a detached managed disk or virtual machine state. Users will need the `Data operator for managed disk` role within Entra ID in order to download a VHD or VM Guest state using a secure URL.

Impact:

In order to apply this setting, the virtual machine to which the disk or disks are attached will need to be powered down and have their disk detached. Users without the `Data operator for managed disk` role within Entra ID will not be able to export VHD or VM Guest state using the secure download URL.

Audit:

Audit from Azure Portal
Part A. Select the Virtual Machine to Evaluate

1. Using the search bar, search for and open the `Virtual Machines` service.
2. Click on the name of the Virtual Machine to be audited.

Part B. Evaluate each Virtual Machine Disk individually

1. From the selected Virtual Machine resource window, expand the `Settings` menu item and click `Disks.`
2. For each disk, click the name of the disk to open the disk resource window.
3. From the selected Disk resource window, expand the `Settings` menu item, and click `Disk Export.`

Ensure that `Enable Data Access Authentication Mode` is `checked`.
Repeat Part B for each Disk attached to a VM.
Repeat Parts A and B to evaluate all Disks in all VMs.

Audit from PowerShell
Run the following command for each disk:

```
Get-AzDisk -ResourceGroupName '<resource_group_name>' -DiskName '<disk_name>'
```

Ensure the `DataAccessAuthMode` setting displays `AzureActiveDirectory` next to it.

Audit from Azure CLI
Run the following command for each disk:

```
az disk show --disk-name ‘<disk_name>’ --resource-group
‘<resource_group_name>’
```

Ensure the `dataAccessAuthMode` setting is set to `AzureActiveDirectory`

Remediation:

Remediate from Azure Portal
Part A. Select the Virtual Machine to Remediate

1. Using the search bar, search for and open the `Virtual Machines` service.
2. Click on the name of the Virtual Machine to be remediated.

Part B. Remediate each Virtual Machine Disk individually

1. From the selected Virtual Machine resource window, expand the `Settings` menu item and click `Disks.`
2. For each disk, click the name of the disk to open the disk resource window.
3. From the selected Disk resource window, expand the `Settings` menu item, and click `Disk Export.`

`check` the checkbox next to `Enable Data Access Authentication Mode`.
Repeat Part B for each Disk attached to a VM.
Repeat Parts A and B to remediate all Disks in all VMs.

Remediate from PowerShell
Ensure that each disk is detached from its associated `Virtual Machine` before proceeding. Once detached, run the following for each disk:

```
$disk = Get-AzDisk -ResourceGroupName '<resource_group_name>' -DiskName
'<disk_name>'
$disk.DataAccessAuthMode = 'AzureActiveDirectory'
Update-AzDisk -ResourceGroup '<resource_group_name>' -DiskName $disk.Name -
Disk $disk
```

Remediate from Azure CLI
Ensure that each disk is detached from its associated `Virtual Machine` before proceeding. Once detached, run the following for each disk:

```
az disk update --name <disk_name> --resource-group <resource_group_name> --
data-access-auth-mode AzureActiveDirectory
```

Default Value:

By default, Data Access Authentication Mode is `Disabled.`

References:

1. https://learn.microsoft.com/en-us/azure/virtual-machines/windows/download-vhd?tabs=azure-portal#secure-downloads-and-uploads-with-microsoft-entra-id
2. https://learn.microsoft.com/en-us/azure/virtual-machines/windows/download-vhd?tabs=azure-portal#secure-downloads-and-uploads-with-microsoft-entra-id

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.6 Securely Manage Enterprise Assets and Software Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

8.7 Ensure that Only Approved Extensions Are Installed (Manual)

Profile Applicability:

- Level 1

Description:

For added security, only install organization-approved extensions on VMs.

Rationale:

Azure virtual machine extensions are small applications that provide post-deployment configuration and automation tasks on Azure virtual machines. These extensions run with administrative privileges and could potentially access anything on a virtual machine. The Azure Portal and community provide several such extensions. Each organization should carefully evaluate these extensions and ensure that only those that are approved for use are actually implemented.

Impact:

Functionality by unsupported extensions will be disabled.

Audit:

Audit from Azure Portal

1. Go to `Virtual machines`.
2. For each virtual machine, click on the server name to select it.
3. In the new column menu, under `Settings` Click on `Extensions + applications`.
4. Ensure that all the listed extensions are approved by your organization for use.

Audit from Azure CLI
Use the below command to list the extensions attached to a VM, and ensure the listed extensions are approved for use.

```
az vm extension list --vm-name <vmName> --resource-group <sourceGroupName> --
query [*].name
```

Audit from PowerShell
Get a list of VMs.

```
Get-AzVM
```

For each VM run the following command.

```
Get-AzVMExtension -ResourceGroupName <VM Resource Group> -VMName <VM Name>
```

Review each `Name`, `ExtensionType`, and `ProvisioningState` to make sure no unauthorized extensions are installed on any virtual machines.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL: https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** c0e996f8-39cf-4af9-9f45-83fbde810432 **- Name:** 'Only approved VM extensions should be installed'

Remediation:

Remediate from Azure Portal

1. Go to `Virtual machines`.
2. For each virtual machine, go to `Settings`.
3. Click on `Extensions + applications`.
4. If there are unapproved extensions, uninstall them.

Remediate from Azure CLI

From the audit command identify the unapproved extensions, and use the below CLI command to remove an unapproved extension attached to VM.

```
az vm extension delete --resource-group <resourceGroupName> --vm-name
<vmName> --name <extensionName>
```

Remediate from PowerShell

For each VM and each insecure extension from the Audit Procedure run the following command.

```
Remove-AzVMExtension -ResourceGroupName <ResourceGroupName> -Name
<ExtensionName> -VMName <VirtualMachineName>
```

Default Value:

By default, no extensions are added to the virtual machines.

References:

1. https://docs.microsoft.com/en-us/azure/virtual-machines/windows/extensions-features
2. https://docs.microsoft.com/en-us/powershell/module/az.compute/?view=azps-7.5.0#vm-extensions
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-asset-management#am-2-use-only-approved-services
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-asset-management#am-5-use-only-approved-applications-in-virtual-machine

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.1 Establish and Maintain a Software Inventory Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	●	●	●
v7	2.1 Maintain Inventory of Authorized Software Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	●	●	●

8.8 Ensure that Endpoint Protection for all Virtual Machines is installed (Manual)

Profile Applicability:

- Level 2

Description:

Install endpoint protection for all virtual machines.

Rationale:

Installing endpoint protection systems (like anti-malware for Azure) provides for real-time protection capability that helps identify and remove viruses, spyware, and other malicious software. These also offer configurable alerts when known-malicious or unwanted software attempts to install itself or run on Azure systems.

Impact:

Endpoint protection will incur an additional cost to you.

Audit:

Audit from Azure Portal

1. Go to `Security Center`
2. Click the `Recommendations` blade
3. Ensure that there are no recommendations for `Endpoint Protection not installed on Azure VMs`

Audit from Azure CLI

```
az vm show -g <MyResourceGroup> -n <MyVm> -d --query
"resources[?type=='Microsoft.Compute/virtualMachines/extensions'].{ExtensionN
ame:name}" -o table
```

If extensions are installed, it will list the installed extensions.

```
EndpointSecurity || TrendMicroDSA* || Antimalware || EndpointProtection ||
SCWPAgent || PortalProtectExtension* || FileSecurity*
```

Alternatively, you can employ your own endpoint protection tool for your OS.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 1f7c564c-0a90-4d44-b7e1-9d456cffaee8 **- Name:** 'Endpoint protection should be installed on your machines'

Remediation:

Follow Microsoft Azure documentation to install endpoint protection from the security center. Alternatively, you can employ your own endpoint protection tool for your OS.

Default Value:

By default Endpoint Protection is disabled.

References:

1. https://docs.microsoft.com/en-us/azure/security-center/security-center-install-endpoint-protection
2. https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware
3. https://docs.microsoft.com/en-us/cli/azure/vm/extension?view=azure-cli-latest#az_vm_extension_list
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-endpoint-security#es-1-use-endpoint-detection-and-response-edr

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.2 Configure Automatic Anti-Malware Signature Updates Configure automatic updates for anti-malware signature files on all enterprise assets.	●	●	●
v7	8.2 Ensure Anti-Malware Software and Signatures are Updated Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.	●	●	●

8.9 [Legacy] Ensure that VHDs are Encrypted (Manual)

Profile Applicability:

- Level 2

Description:

NOTE: This is a legacy recommendation. Managed Disks are encrypted by default and recommended for all new VM implementations.

VHD (Virtual Hard Disks) are stored in blob storage and are the old-style disks that were attached to Virtual Machines. The blob VHD was then leased to the VM. By default, storage accounts are not encrypted, and Microsoft Defender will then recommend that the OS disks should be encrypted. Storage accounts can be encrypted as a whole using PMK or CMK. This should be turned on for storage accounts containing VHDs.

Rationale:

While it is recommended to use Managed Disks which are encrypted by default, "legacy" VHDs may exist for a variety of reasons and may need to remain in VHD format. VHDs are not encrypted by default, so this recommendation intends to address the security of these disks. In these niche cases, VHDs should be encrypted using the procedures in this recommendation to encrypt and protect the data content.

If a virtual machine is using a VHD and can be converted to a managed disk, instructions for this procedure can be found in the resources section of this recommendation under the title "Convert VHD to Managed Disk."

Impact:

Depending on how the encryption is implemented will change the size of the impact. If provider-managed keys(PMK) are utilized, the impact is relatively low, but processes need to be put in place to regularly rotate the keys. If Customer-managed keys(CMK) are utilized, a key management process needs to be implemented to store and manage key rotation, thus the impact is medium to high depending on user maturity with key management.

Audit:

Audit from Azure CLI
For each virtual machine identify if the VM is using a legacy VHD by reviewing the *VHD* parameter in the output of the following command. The *VHD* parameter will contain the Storage Account name used for the VHD.

```
az vm show --name <MyVM> --resource-group <MyResourceGroup>
```

Next, identify if the storage account from the *VHD* parameter is encrypted by reviewing the *encryption --> services --> blob --> enabled* within the output of the following command and make sure its value is *True*.

```
az storage account show --name <storage account name> --resource-group
<resource group>
```

Audit from PowerShell:
Determine whether the VM is using a VHD for the OS Disk and any Data disks.

```
$virtualMachine = Get-AzVM --Name <vm name> --ResourceGroup <resource group
name> |Select-Object -ExpandProperty StorageProfile

$virtualMachine.OsDisk
$virtualMachine.DataDisks
```

Next, use the value from *VHD* to see if the storage blob holding the VHD is encrypted.

```
$storageAccount = Get-AzStorageAccount -Name <storage account name from VHD
setting> -ResourceGroupName <resource group name>

$storageAccount.Encryption.Services.Blob
```

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 702dd420-7fcc-42c5-afe8-4026edd20fe0 **- Name:** 'OS and data disks should be encrypted with a customer-managed key'

Remediation:

Remediate from Azure Portal

1. Navigate to the `storage account` that you wish to encrypt
2. Select `encryption`
3. Select the `encryption type` that you wish to use

If you wish to use a Microsoft-managed key (the default), you can save at this point and encryption will be applied to the account.
If you select `Customer-managed keys`, it will ask for the location of the key (The default is an Azure Key Vault) and the key name.
Once these are captured, save the configuration and the account will be encrypted using the provided key.

Remediate from Azure CLI:
Create the Key Vault

```
az keyvault create --name <name> --resource-group <resourceGroup> --location
<location> --enabled-for-disk-encryption
```

Encrypt the disk and store the key in Key Vault

```
az vm encryption enable -g <resourceGroup> --name <name> --disk-encryption-
keyvault myKV
```

Remediate from PowerShell

This process uses a Key Vault to store the keys

Create the Key Vault

```
New-AzKeyvault -name <name> -ResourceGroupName <resourceGroup> -Location
<location> -EnabledForDiskEncryption
```

Encrypt the disk and store the key in Key Vault

```
$KeyVault = Get-AzKeyVault -VaultName <name> -ResourceGroupName
<resourceGroup>
Set-AzVMDiskEncryptionExtension -ResourceGroupName <resourceGroup> -VMName
<name> -DiskEncryptionKeyVaultUrl $KeyVault.VaultUri -
DiskEncryptionKeyVaultId $KeyVault.ResourceId
```

Default Value:

The default value for encryption is "NO Encryption"

References:

1. CLI: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-cli-quickstart
2. Powershell: https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-powershell-quickstart
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-4-enable-data-at-rest-encryption-by-default
4. Convert VHD to Managed Disk: https://docs.microsoft.com/en-us/previous-versions/azure/virtual-machines/scripts/virtual-machines-powershell-sample-create-managed-disk-from-vhd

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.11 Encrypt Sensitive Data at Rest Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	14.8 Encrypt Sensitive Information at Rest Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

8.10 Ensure only MFA enabled identities can access privileged Virtual Machine (Manual)

Profile Applicability:

- Level 2

Description:

Verify identities without MFA that can log in to a privileged virtual machine using separate login credentials. An adversary can leverage the access to move laterally and perform actions with the virtual machine's managed identity. Make sure the virtual machine only has necessary permissions, and revoke the admin-level permissions according to the least privileges principal

Rationale:

Integrating multi-factor authentication (MFA) as part of the organizational policy can greatly reduce the risk of an identity gaining control of valid credentials that may be used for additional tactics such as initial access, lateral movement, and collecting information. MFA can also be used to restrict access to cloud resources and APIs.

An Adversary may log into accessible cloud services within a compromised environment using Valid Accounts that are synchronized to move laterally and perform actions with the virtual machine's managed identity. The adversary may then perform management actions or access cloud-hosted resources as the logged-on managed identity.

Impact:

This recommendation requires the Entra ID P2 license to implement.

Ensure that identities that are provisioned to a virtual machine utilizes an RBAC/ABAC group and is allocated a role using Azure PIM, and the Role settings require MFA or use another third-party PAM solution for accessing Virtual Machines.

Audit:

Audit from Azure Portal

1. Log in to the Azure portal.
2. Select the `Subscription`, then click on `Access control (IAM)`.
3. Select `Role Assignments` from the top menu and apply filters on `Assignment type` as `Privileged administrator roles` and `Type` as `Virtual Machines`.
4. Verify the list of privileged managed identities attached to any virtual machine.
5. If there are privileged managed identities from the above list, then check the list of users without MFA by navigating to `Entra ID`.
6. In the left navigation pane select `Users` from `Manage`.
7. Click on `Per-User MFA` from the top menu options and for each user with `MULTI-FACTOR AUTH STATUS` as `Disabled` follow the below-mentioned steps:

        - Select the `Subscription`, then click on `Access control (IAM)`.
        - Select `Check access` and click on `User, group, or service principal`.
        - Enter the username or email and verify there are no role assignments on the user that provides access like `Virtual Machine Administrator Login` or `Virtual Machine User Login`. Make sure this follows the least privileges principal.

Remediation:

Remediate from Azure Portal

1. Log in to the Azure portal.
2. This can be remediated by enabling MFA for user, Removing user access or Reducing access of managed identities attached to virtual machines.

- Case I : Enable MFA for users having access on virtual machines.
    1. Navigate to `Entra ID` from the left pane and select `Users` from the `Manage` section.
    2. Click on `Per-User MFA` from the top menu options and select each user with `MULTI-FACTOR AUTH STATUS` as `Disabled` and can login to virtual machines:
        - From `quick steps` on the right side select `enable`.
        - Click on `enable multi-factor auth` and share the link with the user to setup MFA as required.
- Case II : Removing user access on a virtual machine.
    1. Select the `Subscription`, then click on `Access control (IAM)`.
    2. Select `Role assignments` and search for `Virtual Machine Administrator Login` or `Virtual Machine User Login` or any role that provides access to log into virtual machines.
    3. Click on `Role Name`, Select `Assignments`, and remove identities with no MFA configured.
- Case III : Reducing access of managed identities attached to virtual machines.
    1. Select the `Subscription`, then click on `Access control (IAM)`.
    2. Select `Role Assignments` from the top menu and apply filters on `Assignment type` as `Privileged administrator roles` and `Type` as `Virtual Machines`.
    3. Click on `Role Name`, Select `Assignments`, and remove identities access make sure this follows the least privileges principal.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	6.5 Require MFA for Administrative Access Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	4.5 Use Multifactor Authentication For All Administrative Access Use multi-factor authentication and encrypted channels for all administrative account access.		●	●

8.11 Ensure Trusted Launch is enabled on Virtual Machines (Automated)

Profile Applicability:

- Level 1

Description:

When **Secure Boot** and **vTPM** are enabled together, they provide a strong foundation for protecting your VM from boot attacks. For example, if an attacker attempts to replace the bootloader with a malicious version, Secure Boot will prevent the VM from booting. If the attacker is able to bypass Secure Boot and install a malicious bootloader, vTPM can be used to detect the intrusion and alert you.

Rationale:

Secure Boot and vTPM work together to protect your VM from a variety of boot attacks, including bootkits, rootkits, and firmware rootkits. Not enabling Trusted Launch in Azure VM can lead to increased vulnerability to rootkits and boot-level malware, reduced ability to detect and prevent unauthorized changes to the boot process, and a potential compromise of system integrity and data security.

Impact:

Secure Boot and vTPM are not currently supported for Azure Generation 1 VMs.

IMPORTANT: Before enabling Secure Boot and vTPM on a Generation 2 VM which does not already have both enabled, it is highly recommended to create a restore point of the VM prior to remediation.

Audit:

Audit from Azure Portal

1. Go to Virtual Machines
2. For each VM, under Settings, click on Configuration on the left blade
3. Under Security Type, make sure security type is not standard and if it is Trusted Launch Virtual Machines then make sure Enable Secure Boot & Enable vTPM are checked

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 97566dd7-78ae-4997-8b36-1c7bfe0d8121 **- Name:** '[Preview]: Secure Boot should be enabled on supported Windows virtual machines'

Remediation:

Remediate from Azure Portal

1. Go to Virtual Machines.
2. For each VM, under Settings, click on Configuration on the left blade.
3. Under Security Type, select 'Trusted Launch Virtual Machines'.
4. Make sure Enable Secure Boot & Enable vTPM are checked.
5. Click on Apply.

Note: Trusted launch on existing virtual machines (VMs) is currently not supported for Azure Generation 1 VMs

Default Value:

On Azure Generation 2 VMs, vTPM is enabled by default. Secure Boot is not enabled by default.

References:

1. https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch-existing-vm?tabs=portal
2. https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch-existing-vm?tabs=portal#enable-trusted-launch-on-existing-vm
3. https://learn.microsoft.com/en-us/azure/virtual-machines/trusted-launch#secure-boot

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	4.1 Establish and Maintain a Secure Configuration Process Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	5.1 Establish Secure Configurations Maintain documented, standard security configuration standards for all authorized operating systems and software.	●	●	●

9 AppService

This section covers security recommendations for Azure AppService.

9.1 Ensure 'HTTPS Only' is set to `On` (Automated)

Profile Applicability:

- Level 1

Description:

Azure App Service allows apps to run under both HTTP and HTTPS by default. Apps can be accessed by anyone using non-secure HTTP links by default. Non-secure HTTP requests can be restricted and all HTTP requests redirected to the secure HTTPS port. It is recommended to enforce HTTPS-only traffic.

Rationale:

Enabling HTTPS-only traffic will redirect all non-secure HTTP requests to HTTPS ports. HTTPS uses the TLS/SSL protocol to provide a secure connection which is both encrypted and authenticated. It is therefore important to support HTTPS for the security benefits.

Impact:

When it is enabled, every incoming HTTP request is redirected to the HTTPS port. This means an extra level of security will be added to the HTTP requests made to the app.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. For each App Service
4. Under `Setting` section, click on `Configuration`
5. Under the `General Settings` tab, ensure that `HTTPS Only` is set to `On` under `Platform Settings`

Audit from Azure CLI
To check HTTPS-only traffic value for an existing app, run the following command,

```
az webapp show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --
query httpsOnly
```

The output should return `true` if HTTPS-only traffic value is set to `On`.

Audit from PowerShell
List all the web apps configured within the subscription.

```
Get-AzWebApp | Select-Object ResourceGroup, Name, HttpsOnly
```

For each web app review the `HttpsOnly` setting and make sure it is set to `True`.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL: https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** a4af4a39-4135-47fb-b175-47fbdf85311d **- Name:** 'App Service apps should only be accessible over HTTPS'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. For each App Service
4. Under `Setting` section, click on `Configuration`
5. Under the `General Settings` tab, set `HTTPS Only` to `On` under `Platform Settings`

Remediate from Azure CLI

To set HTTPS-only traffic value for an existing app, run the following command:

```
az webapp update --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --
set httpsOnly=true
```

Remediate from PowerShell

```
Set-AzWebApp -ResourceGroupName <RESOURCE_GROUP_NAME> -Name <APP_NAME> -
HttpsOnly $true
```

Default Value:

By default, HTTPS-only feature will be disabled when a new app is created using the command-line tool or Azure Portal console.

References:

1. https://learn.microsoft.com/en-us/azure/app-service/overview-security?source=recommendations#https-and-certificates
2. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-3-encrypt-sensitive-data-in-transit
3. https://learn.microsoft.com/en-us/powershell/module/az.websites/set-azwebapp
4. https://techcommunity.microsoft.com/t5/azure-paas-blog/enable-https-setting-on-azure-app-service-using-azure-policy/ba-p/3286603

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

9.2 Ensure App Service Authentication is set up for apps in Azure App Service (Automated)

Profile Applicability:

- Level 2

Description:

Azure App Service Authentication is a feature that can prevent anonymous HTTP requests from reaching a Web Application or authenticate those with tokens before they reach the app. If an anonymous request is received from a browser, App Service will redirect to a logon page. To handle the logon process, a choice from a set of identity providers can be made, or a custom authentication mechanism can be implemented.

Rationale:

By Enabling App Service Authentication, every incoming HTTP request passes through it before being handled by the application code. It also handles authentication of users with the specified provider (Entra ID, Facebook, Google, Microsoft Account, and Twitter), validation, storing and refreshing of tokens, managing the authenticated sessions and injecting identity information into request headers. Disabling HTTP Basic Authentication functionality further ensures legacy authentication methods are disabled within the application.

Impact:

This is only required for App Services which require authentication. Enabling on site like a marketing or support website will prevent unauthenticated access which would be undesirable.

Adding Authentication requirement will increase cost of App Service and require additional security components to facilitate the authentication.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under `Settings` section, Click on `Authentication`
5. Ensure that `App Service authentication` set to `Enabled` (Will only appear once an Identity provider is set up/selected)
6. Navigate back to the application blade
7. Under `Settings`, click on `Configuration`
8. Click on the 'General Settings' tab

9. Under `Platform settings`, ensure `Basic Auth Publishing Credentials` is set to `Off`

Audit from Azure CLI

To check App Service Authentication status for an existing app, run the following command (using authV1 extension),

```
az webapp auth show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
--query enabled
```

The output should return `true` if App Service authentication is set to `On`.

If using the `authV2` extension for the `az webapp auth` CLI, run the following command,

```
az webapp auth show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
```

Ensure that the `enabled` setting under `platform` is set to `true`.

To check whether the `Basic Auth Publishing Credentials` are disabled, issue the following commands,

```
az resource show --resource-group <RESOURCE GROUP NAME> --name scm --
namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --
parent sites/<APPLICATION NAME>

az resource show --resource-group <RESOURCE GROUP NAME> --name ftp --
namespace Microsoft.Web --resource-type basicPublishingCredentialsPolicies --
parent sites/<APPLICATION NAME>
```

Ensure `allow` is set to `false` under `properties` within the output of each of the above commands.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:

https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** c75248c1-ea1d-4a9c-8fc9-29a6aabd5da8 **- Name:** 'Function apps should have authentication enabled'
- **Policy ID:** 95bccee9-a7f8-4bec-9ee9-62c3473701fc **- Name:** 'App Service apps should have authentication enabled'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under `Setting` section, click on `Authentication`
5. If no identity providers are set up, then click `Add identity provider`
6. Choose other parameters as per your requirements and click on `Add`

To disable the `Basic Auth Publishing Credentials` setting, perform the following steps:

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under `Settings`, click on `Configuration`
5. Click on the 'General Settings' tab
6. Under `Platform settings`, ensure `Basic Auth Publishing Credentials` is set to `Off`

Remediate from Azure CLI

To set App Service Authentication for an existing app, run the following command:

```
az webapp auth update --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME> --enabled true
```

Note

In order to access `App Service authentication` settings for Web app using Microsoft API requires `Website contributor` permission at subscription level. A custom role can be created in place of `Website contributor` to provide more specific permission and maintain the principle of least privileged access.

Default Value:

By default, App Service Authentication is disabled when a new app is created using the command-line tool or Azure Portal console.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/app-service-authentication-overview
2. https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#website-contributor
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-privileged-access#pa-3-manage-lifecycle-of-identities-and-entitlements
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-governance-strategy#gs-6-define-and-implement-identity-and-privileged-access-strategy

Additional Information:

You're not required to use App Service for authentication and authorization. Many web frameworks are bundled with security features, and you can use them if you like. If you need more flexibility than App Service provides, you can also write your own utilities. Secure authentication and authorization require deep understanding of security, including federation, encryption, JSON web tokens (JWT) management, grant types, and so on.

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user’s need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

9.3 Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled' (Automated)

Profile Applicability:

- Level 1

Description:

By default, App Services can be deployed over FTP. If FTP is required for an essential deployment workflow, FTPS should be required for FTP login for all App Services.

If FTPS is not expressly required for the App, the recommended setting is `Disabled.`

Rationale:

FTP is an unencrypted network protocol that will transmit data - including passwords - in clear-text. The use of this protocol can lead to both data and credential compromise, and can present opportunities for exfiltration, persistence, and lateral movement.

Impact:

Any deployment workflows that rely on FTP or FTPs rather than the WebDeploy or HTTPs endpoints may be affected.

Audit:

Audit from Azure Portal

1. Go to the Azure Portal
2. Select `App Services`
3. Click on an app
4. Select `Settings` and then `Configuration`
5. Under `General Settings`, for the `Platform Settings`, the `FTP state` should not be set to `All allowed`

Audit from Azure CLI
List webapps to obtain the ids.

```
az webapp list
```

List the publish profiles to obtain the username, password
and ftp server url.

```
az webapp deployment list-publishing-profiles --ids <ids>
{
  "publishUrl": <URL_FOR_WEB_APP>,
    "userName": <USER_NAME>,
    "userPWD": <USER_PASSWORD>,
}
```

Audit from PowerShell

List all Web Apps:

```
Get-AzWebApp
```

For each app:

```
Get-AzWebApp -ResourceGroupName <resource group name> -Name <app name> |
Select-Object -ExpandProperty SiteConfig
```

In the output, look for the value of **FtpsState**. If its value is **AllAllowed** the setting is out of compliance. Any other value is considered in compliance with this check.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.

If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 399b2637-a50f-4f95-96f8-3a145476eb15 **- Name:** 'Function apps should require FTPS only'
- **Policy ID:** 4d24b6d4-5e53-4a4f-a7f4-618fa573ee4b **- Name:** 'App Service apps should require FTPS only'

Remediation:

Remediate from Azure Portal

1. Go to the Azure Portal
2. Select `App Services`
3. Click on an app
4. Select `Settings` and then `Configuration`
5. Under `General Settings`, for the `Platform Settings`, the `FTP state` should be set to `Disabled` or `FTPS Only`

Remediate from Azure CLI

For each out of compliance application, run the following choosing either 'disabled' or 'FtpsOnly' as appropriate:

```
az webapp config set --resource-group <resource group name> --name <app name>
--ftps-state [disabled|FtpsOnly]
```

Remediate from PowerShell

For each out of compliance application, run the following:

```
Set-AzWebApp -ResourceGroupName <resource group name> -Name <app name> -
FtpsState <Disabled or FtpsOnly>
```

Default Value:

By default, FTP based deployment is `All allowed`

References:

1. https://docs.microsoft.com/en-us/azure/app-service/deploy-ftp
2. https://docs.microsoft.com/en-us/azure/app-service/overview-security
3. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-encrypt-sensitive-information-in-transit
4. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities
5. https://learn.microsoft.com/en-us/rest/api/appservice/web-apps/create-or-update-configuration#ftpsstate

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●
v7	16.5 Encrypt Transmittal of Username and Authentication Credentials Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

9.4 Ensure Web App is using the latest version of TLS encryption (Automated)

Profile Applicability:

- Level 1

Description:

The TLS (Transport Layer Security) protocol secures transmission of data over the internet using standard encryption technology. Encryption should be set with the latest version of TLS. App service allows TLS 1.2 by default, which is the recommended TLS level by industry standards such as PCI DSS.

Rationale:

App service currently allows the web app to set TLS versions 1.0, 1.1 and 1.2. It is highly recommended to use the latest TLS 1.2 version for web app secure connections.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under `Setting` section, Click on `TLS/SSL settings`
5. Under the `Bindings` pane, ensure that `Minimum TLS Version` set to `1.2` under `Protocol Settings`

Audit from Azure CLI

To check TLS Version for an existing app, run the following command,

```
az webapp config show --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME> --query minTlsVersion
```

The output should return `1.2` if TLS Version is set to `1.2` (Which is currently the latest version).

Audit from PowerShell

List all web apps.

```
Get-AzWebApp
```

For each web app run the following command.

```
Get-AzWebApp -ResourceGroupName <RESOURCE_GROUP_NAME> -Name <APP_NAME>
|Select-Object -ExpandProperty SiteConfig
```

Make sure the `minTlsVersion` is set to at least `1.2`.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** f9d614c5-c173-4d56-95a7-b4437057d193 **- Name:** 'Function apps should use the latest TLS version'
- **Policy ID:** f0e6e85b-9b9f-4a4b-b67b-f730d42f1b0b **- Name:** 'App Service apps should use the latest TLS version'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under `Setting` section, Click on `SSL settings`
5. Under the `Bindings` pane, set `Minimum TLS Version` to `1.2` under `Protocol Settings` section

Remediate from Azure CLI

To set TLS Version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
--min-tls-version 1.2
```

Remediate from PowerShell

```
Set-AzWebApp -ResourceGroupName <RESOURCE_GROUP_NAME> -Name <APP_NAME> -
MinTlsVersion 1.2
```

Default Value:

By default, TLS Version feature will be set to 1.2 when a new app is created using the command-line tool or Azure Portal console.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-ssl#enforce-tls-versions
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-data-protection#dp-3-encrypt-sensitive-data-in-transit
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-network-security#ns-8-detect-and-disable-insecure-services-and-protocols
4. https://docs.microsoft.com/en-us/powershell/module/az.websites/set-azwebapp?view=azps-8.1.0

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.10 Encrypt Sensitive Data in Transit Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	14.4 Encrypt All Sensitive Information in Transit Encrypt all sensitive information in transit.		●	●

9.5 Ensure that Register with Entra ID is enabled on App Service (Automated)

Profile Applicability:

- Level 1

Description:

Managed service identity in App Service provides more security by eliminating secrets from the app, such as credentials in the connection strings. When registering an App Service with Entra ID, the app will connect to other Azure services securely without the need for usernames and passwords.

Rationale:

App Service provides a highly scalable, self-patching web hosting service in Azure. It also provides a managed identity for apps, which is a turn-key solution for securing access to Azure SQL Database and other Azure services.

Audit:

Audit from Azure Portal

1. From Azure Portal open the Portal Menu in the top left
2. Go to `App Services`
3. Click on each App
4. Under the `Setting` section, Click on `Identity`
5. Under the `System assigned` pane, ensure that `Status` set to `On`

Audit from Azure CLI
To check Register with Entra ID feature status for an existing app, run the following command,

```
az webapp identity show --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME> --query principalId
```

The output should return unique Principal ID.
If no output for the above command then Register with Entra ID is not set.
Audit from PowerShell
List the web apps.

```
Get-AzWebApp
```

For each web app run the following command.

```
Get-AzWebapp -ResourceGroupName  <app resource group> -Name <app name>
```

Make sure the `Identity` setting contains a unique Principal ID

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 0da106f2-4ca3-48e8-bc85-c638fe6aea8f **- Name:** 'Function apps should use managed identity'
- **Policy ID:** 2b9ad585-36bc-4615-b300-fd4435808332 **- Name:** 'App Service apps should use managed identity'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under `Setting` section, Click on `Identity`
5. Under the `System assigned` pane, set `Status` to `On`

Remediate from Azure CLI

To register with Entra ID for an existing app, run the following command:

```
az webapp identity assign --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME>
```

Remediate from PowerShell

To register with Entra ID for an existing app, run the following command:

```
Set-AzWebApp -AssignIdentity $True -ResourceGroupName <resource_Group_Name> -
Name <App_Name>
```

Default Value:

By default, Managed service identity via Entra ID is disabled.

References:

1. https://docs.microsoft.com/en-gb/azure/app-service/app-service-web-tutorial-connect-msi
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-1-use-centralized-identity-and-authentication-system

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

9.6 Ensure that 'Basic Authentication' is 'Disabled' (Manual)

Profile Applicability:

- Level 1

Description:

Basic Authentication provides the ability to create identities and authentication for an App Service without a centralized Identity Provider. For a more effective, capable, and secure solution for Identity, Authentication, Authorization, and Accountability, a centralized Identity Provider such as Entra ID is strongly advised.

Rationale:

Basic Authentication introduces an identity silo which can produce privileged access to a resource. This can be exploited in numerous ways and represents a significant vulnerability and attack vector.

Impact:

An Identity Provider that can be used by the App Service for authenticating users is required.

Audit:

Audit from Azure Portal

1. Search for, and open `App Services` from the search bar.
2. For each App Service listed:
3. Click on the App Service name.
4. Under the `Settings` menu item, click on `Configuration`
5. Under the `General settings` tab, scroll down to locate the two Basic Auth settings:
    - `SCM Basic Auth Publishing Credentials`
    - `FTP Basic Auth Publishing Credentials`

Both radio buttons should indicate a status of `Off.`
Repeat this procedure for each App Service.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 871b205b-57cf-4e1e-a234-492616998bf7 **- Name:** 'App Service apps should have local authentication methods disabled for FTP deployments'
- **Policy ID:** aede300b-d67f-480a-ae26-4b3dfb1a1fdc **- Name:** 'App Service apps should have local authentication methods disabled for SCM site deployments'

Remediation:

Remediate from Azure Portal

1. Search for, and open `App Services` from the search bar.
2. For each App Service listed:
3. Click on the App Service name.
4. Under the `Settings` menu item, click on `Configuration`
5. Under the `General settings` tab, scroll down to locate the two Basic Auth settings:

- Set the `SCM Basic Auth Publishing Credentials` radio button to `Off`
- Set the `FTP Basic Auth Publishing Credentials` radio button to `Off`

CAUTION: The new settings are not yet applied. Applying them may cause your App Service resource to restart - proceed with caution. Click the `Save` button, then click `Continue` to apply the updated configuration.
Repeat this procedure for each App Service.

Default Value:

Both parameters for Basic Authentication (SCM and FTP) are set to `On` by default.

References:

1. https://learn.microsoft.com/en-us/azure/app-service/configure-basic-auth-disable?tabs=portal

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.6 Centralize Account Management Centralize account management through a directory or identity service.		●	●
v7	16.2 Configure Centralized Point of Authentication Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

9.7 Ensure that 'PHP version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of PHP may be deprecated and no longer supported. Using a supported version of PHP for app services is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of the currently supported versions of PHP here:
https://www.php.net/supported-versions.php
Audit from Azure Portal

1. From Azure Home open the Portal Menu in the top left
2. Go to `App Services`
3. Click on each App
4. Under `Settings` section, click on `Configuration`
5. Click on the `General settings` pane, ensure that for a `Stack` of `PHP` the `Major Version` and `Minor Version` reflect a currently supported release.

NOTE: No action is required If `PHP version` is set to `Off` as PHP is not used by your web app.

Audit from Azure CLI
To check PHP version for an existing app, run the following command,

```
az webapp config show --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME> --query "{LinuxFxVersion:linuxFxVersion,PHP_Version:phpVersion}"
```

The output should return a currently supported version of PHP. Any other version of PHP would be considered a finding.
NOTE: No action is required if the output is empty, as PHP is not used by your app.

Audit from PowerShell

```
$application = Get-AzWebApp -ResourceGroupName <RESOURCE_GROUP_NAME> -Name
<APP_NAME>
$application.SiteConfig | select-object LinuxFXVersion, phpVersion
```

The output should return a currently supported version of PHP. Any other version of PHP would be considered a finding.
NOTE: No action is required if the output is empty, as PHP is not used by your app.

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** f466b2a6-823d-470d-8ea5-b031e72d79ae **- Name:** 'App Service app slots that use PHP should use a specified 'PHP version''
- **Policy ID:** 7261b898-8a84-4db8-9e04-18527132abb3 **- Name:** 'App Service apps that use PHP should use a specified 'PHP version''

Remediation:

Remediate from Azure Portal

1. From Azure Home open the Portal Menu in the top left
2. Go to `App Services`
3. Click on each App
4. Under `Settings` section, click on `Configuration`
5. Click on the `General settings` pane, ensure that for a `Stack` of `PHP` the `Major Version` and `Minor Version` reflect a currently supported release.

NOTE: No action is required If `PHP version` is set to `Off` or is set with an empty value as PHP is not used by your app.

Remediate from Azure CLI

List the available PHP runtimes:

```
az webapp list-runtimes
```

To set a currently supported PHP version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
[--linux-fx-version <PHP_RUNTIME_VERSION>][--php-version <PHP_VERSION>]
```

Remediate from PowerShell

To set a currently supported PHP version for an existing app, run the following command:

```
Set-AzWebApp -ResourceGroupName <RESOURCE_GROUP_NAME> -Name <APP_NAME> -
phpVersion <PHP_VERSION>
```

NOTE: Currently there is no way to update an existing web app `Linux FX Version` setting using PowerShell, nor is there a way to create a new web app using PowerShell that configures the PHP runtime in the `Linux FX Version` setting.

Default Value:

The version of PHP is whatever was selected upon App creation.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings
2. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities
3. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources
4. https://www.php.net/supported-versions.php

Additional Information:

Currently supported versions can be confirmed here: https://www.php.net/supported-versions.php

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 Ensure Authorized Software is Currently Supported Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	●	●	●
v7	2.2 Ensure Software is Supported by Vendor Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	●	●	●

9.8 Ensure that 'Python version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of Python may be deprecated and no longer supported. Using a supported version of Python for app services is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of the currently supported versions (given a status of "security") of Python here: https://devguide.python.org/versions/
Audit from Azure Portal

1. From Azure Home open the Portal Menu in the top left
2. Go to `App Services`
3. Click on each App
4. Under `Settings` section, click on `Configuration`
5. Click on the General settings pane and ensure that for a Stack of Python the Major version and Minor version reflect a currently supported release

NOTE: No action is required if `Python version` is set to `Off`, as Python is not used by your app.
Audit from Azure CLI
To check Python version for an existing app, run the following command

```
az webapp config show --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME> --query
"{LinuxFxVersion:linuxFxVersion,WindowsFxVersion:windowsFxVersion,PythonVersi
on:pythonVersion}"
```

The output should return a currently supported version of Python.
NOTE: No action is required if the output is empty, as Python is not used by your app.

Audit from PowerShell

```
$app = Get-AzWebApp -Name <APP_NAME> -ResourceGroup <RESOURCE_GROUP_NAME>
$app.SiteConfig |Select-Object LinuxFXVersion, WindowsFxVersion,
PythonVersion
```

Ensure the output of the above command shows a currently supported of Python.
NOTE: No action is required if the output is empty, as Python is not used by your app.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** 9c014953-ef68-4a98-82af-fd0f6b2306c8 **- Name:** 'App Service app slots that use Python should use a specified 'Python version''
- **Policy ID:** 7008174a-fd10-4ef0-817e-fc820a951d73 **- Name:** 'App Service apps that use Python should use a specified 'Python version''

Remediation:

Remediate from Azure Portal

1. From Azure Home open the Portal Menu in the top left
2. Go to `App Services`
3. Click on each App
4. Under `Settings` section, click on `Configuration`
5. Click on the General settings pane and ensure that the Major Version and the Minor Version is set to a currently supported release.

NOTE: No action is required if `Python version` is set to `Off`, as Python is not used by your app.
Remediate from Azure CLI
To see the list of supported runtimes:

```
az webapp list-runtimes
```

To set latest Python version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
[--windows-fx-version "PYTHON|<VERSION>"] [--linux-fx-version
"PYTHON|<VERSION>"]
```

Remediate from PowerShell
As of this writing, there is no way to update an existing application's `SiteConfig` or set a new application's `SiteConfig` settings during creation via PowerShell.

Default Value:

The version of Python is whatever was selected upon App creation.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings
2. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities
3. https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources
4. https://devguide.python.org/versions/

Additional Information:

Currently supported versions of Python can be confirmed by going to https://devguide.python.org/versions/. The currently supported versions are given the status of "security."

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 Ensure Authorized Software is Currently Supported Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	●	●	●
v7	2.2 Ensure Software is Supported by Vendor Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	●	●	●

9.9 Ensure that 'Java version' is currently supported (if in use) (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, older versions of Java may be deprecated and no longer supported. Using a supported version of Java for app services is recommended to avoid potential unpatched vulnerabilities.

Rationale:

Deprecated and unsupported versions of programming and scripting languages can present vulnerabilities which may not be addressed or may not be addressable.

Impact:

If your app is written using version-dependent features or libraries, they may not be available on more recent versions. If you wish to update, research the impact thoroughly.

Audit:

Take note of currently supported version of Java here:
https://www.oracle.com/java/technologies/java-se-support-roadmap.html
Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under `Settings` section, click on `Configuration`
5. Click on the `General settings` pane and ensure that for a `Stack` of `Java` the `Major Version` and `Minor Version` reflect a currently supported release, and that the `Java web server version` is set to the `auto-update` option.

NOTE: No action is required if `Java version` is set to `Off`, as Java is not used by your app.

Audit from Azure CLI
To check Java version for an existing app, run the following command,

```
az webapp config show --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME> --query "{LinuxFxVersion:linuxFxVersion,
WindowsFxVersion:windowsFxVersion, JavaVersion:javaVersion,
JavaContainerVersion:javaContainerVersion, JavaContainer:javaContainer}"
```

Ensure the Java version used within the application is a currently supported version (if java is being used for the app being audited).

Audit from PowerShell

For each application, store the application information within an object, and then interrogate the `SiteConfig` information for that application object.

```
$app = Get-AzWebApp -Name <APP_NAME> -ResourceGroup <RESOURCE_GROUP_NAME>

$app.SiteConfig |Select-Object LinuxFXVersion, WindowsFxVersion, JavaVersion,
JavaContainerVersion, JavaContainer
```

Ensure the Java version used within the application is a currently supported version (if Java is being used for the app being audited).

Audit from Azure Policy

If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** e1d1b522-02b0-4d18-a04f-5ab62d20445f **- Name:** 'Function app slots that use Java should use a specified 'Java version''
- **Policy ID:** 9d0b6ea4-93e2-4578-bf2f-6bb17d22b4bc **- Name:** 'Function apps that use Java should use a specified 'Java version''

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under `Settings` section, click on `Configuration`
5. Click on the `General settings` pane and ensure that for a `Stack` of `Java` the `Major Version` and `Minor Version` reflect a currently supported release, and that the `Java web server version` is set to the `auto-update` option.

NOTE: No action is required if `Java version` is set to `Off`, as Java is not used by your app.

Remediate from Azure CLI

To see the list of supported runtimes:

```
az webapp list-runtimes
```

To set a currently supported Java version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
[--java-version <JAVA_VERSION> --java-container <JAVA_CONTAINER> --java-
container-version <JAVA_CONTAINER_VERSION> [--windows-fx-version
<JAVA_RUNTIME_VERSION>] [--linux-fx-version <JAVA_RUNTIME_VERSION>]
```

If creating a new application to use a currently supported version of Java, run the following commands.
To create an app service plan:

```
az appservice plan create --resource-group <RESOURCE_GROUP_NAME> --name
<PLAN_NAME> --location <LOCATION> [--is-linux --number-of-workers <INT> --sku
<PRICING_TIER>] [--hyper-v --sku <PRICING_TIER>]
```

Get the app service plan ID:

```
az appservice plan list --query "[].{Name:name, ID:id, SKU:sku,
Location:location}"
```

To create a new Java web application using the retrieved app service ID:

```
az webapp create --resource-group <RESOURCE_GROUP_NAME> --plan
<APP_SERVICE_PLAN_ID> --name <app name> [--linux-fx-version
<JAVA_RUNTIME_VERSION>] [--windows-fx-version <JAVA_RUNTIME_VERSION>]
```

Remediate from PowerShell
As of this writing, there is no way to update an existing application's `SiteConfig` or set a new application's `SiteConfig` settings during creation via PowerShell.

Default Value:

The default setting is whichever setting was chosen in the creation of the webapp.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-3-define-and-establish-secure-configurations-for-compute-resources
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-6-rapidly-and-automatically-remediate-vulnerabilities
4. https://www.oracle.com/java/technologies/java-se-support-roadmap.html

Additional Information:

Take note of currently supported version of Java here:
https://www.oracle.com/java/technologies/java-se-support-roadmap.html

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 Ensure Authorized Software is Currently Supported Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise’s mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	●	●	●
v7	2.2 Ensure Software is Supported by Vendor Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	●	●	●

9.10 Ensure that 'HTTP20enabled' is set to 'true' (if in use) (Automated)

Profile Applicability:

- Level 1

Description:

Periodically, newer versions are released for HTTP either due to security flaws or to include additional functionality. Using the latest HTTP version for apps to take advantage of security fixes, if any, and/or new functionalities of the newer version.

Rationale:

Newer versions may contain security enhancements and additional functionality. Using the latest version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected.

HTTP 2.0 has additional performance improvements on the head-of-line blocking problem of old HTTP version, header compression, and prioritization of requests. HTTP 2.0 no longer supports HTTP 1.1's chunked transfer encoding mechanism, as it provides its own, more efficient, mechanisms for data streaming.

Impact:

Most modern browsers support HTTP 2.0 protocol over TLS only, while non-encrypted traffic continues to use HTTP 1.1. To ensure that client browsers connect to your app with HTTP/2, either buy an App Service Certificate for your app's custom domain or bind a third-party certificate.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under `Setting` section, Click on `Configuration`
5. Ensure that `HTTP Version` set to `2.0` version under `General settings`

NOTE: Most modern browsers support HTTP 2.0 protocol over TLS only, while non-encrypted traffic continues to use HTTP 1.1. To ensure that client browsers connect to your app with HTTP/2, either buy an App Service Certificate for your app's custom domain or bind a third-party certificate.

Audit from Azure CLI
To check HTTP 2.0 version status for an existing app, run the following command,

```
az webapp config show --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME> --query http20Enabled
```

The output should return `true` if HTTPS 2.0 traffic value is set to `On`.

Audit from PowerShell
For each application, run the following command:

```
Get-AzWebApp -ResourceGroupName <app resource group> -Name <app name>
|Select-Object -ExpandProperty SiteConfig
```

If the value of the **Http20Enabled** setting is **true**, the application is compliant. Otherwise if the value of the **Http20Enabled** setting is **false**, the application is non-compliant.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** e2c1c086-2d84-4019-bff3-c44ccd95113c **- Name:** 'Function apps should use latest 'HTTP Version''
- **Policy ID:** 8c122334-9d20-4eb8-89ea-ac9a705b74ae **- Name:** 'App Service apps should use latest 'HTTP Version''

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under `Setting` section, Click on `Configuration`
5. Set `HTTP version` to `2.0` under `General settings`

NOTE: Most modern browsers support HTTP 2.0 protocol over TLS only, while non-encrypted traffic continues to use HTTP 1.1. To ensure that client browsers connect to your app with HTTP/2, either buy an App Service Certificate for your app's custom domain or bind a third-party certificate.

Remediate from Azure CLI
To set HTTP 2.0 version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
--http20-enabled true
```

Remediate from PowerShell
To enable HTTP 2.0 version support, run the following command:

```
Set-AzWebApp -ResourceGroupName <app resource group> -Name <app name> -
Http20Enabled $true
```

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-3-define-and-establish-secure-configurations-for-compute-resources
3. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-6-rapidly-and-automatically-remediate-vulnerabilities

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	2.2 Ensure Authorized Software is Currently Supported Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.	●	●	●
v7	2.2 Ensure Software is Supported by Vendor Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.	●	●	●

9.11 Ensure Azure Key Vaults are Used to Store Secrets (Manual)

Profile Applicability:

- Level 2

Description:

Azure Key Vault will store multiple types of sensitive information such as encryption keys, certificate thumbprints, and Managed Identity Credentials. Access to these 'Secrets' can be controlled through granular permissions.

Rationale:

The credentials given to an application have permissions to create, delete, or modify data stored within the systems they access. If these credentials are stored within the application itself, anyone with access to the application or a copy of the code has access to them. Storing within Azure Key Vault as secrets increases security by controlling access. This also allows for updates of the credentials without redeploying the entire application.

Impact:

Integrating references to secrets within the key vault are required to be specifically integrated within the application code. This will require additional configuration to be made during the writing of an application, or refactoring of an already written one. There are also additional costs that are charged per 10000 requests to the Key Vault.

Audit:

Audit from Azure Portal

1. Login to Azure Portal.
2. In the expandable menu on the left go to `Key Vaults`.
3. View the Key Vaults listed.

Audit from Azure CLI

To list key vaults within a subscription run the following command:

```
Get-AzKeyVault
```

To list the secrets within these key vaults run the following command:

```
Get-AzKeyVaultSecret [-VaultName] <vault name>
```

Audit from PowerShell

To list key vaults within a subscription run the following command:

```
Get-AzKeyVault
```

To list all secrets in a key vault run the following command:

```
Get-AzKeyVaultSecret -VaultName '<vaultName'
```

Remediation:

Remediation has 2 steps

1. Setup the Key Vault
2. Setup the App Service to use the Key Vault

Step 1: Set up the Key Vault
Remediate from Azure CLI

```
az keyvault create --name "<name>" --resource-group "<myResourceGroup>" --
location myLocation
```

Remediate from PowerShell

```
New-AzKeyvault -name <name> -ResourceGroupName <myResourceGroup> -Location
<myLocation>
```

Step 2: Set up the App Service to use the Key Vault
Sample JSON Template for App Service Configuration (starting next page):

```
{
    //...
    "resources": [
        {
            "type": "Microsoft.Storage/storageAccounts",
            "name": "[variables('storageAccountName')]",
            //...
        },
        {
            "type": "Microsoft.Insights/components",
            "name": "[variables('appInsightsName')]",
            //...
        },
        {
            "type": "Microsoft.Web/sites",
            "name": "[variables('functionAppName')]",
            "identity": {
                "type": "SystemAssigned"
            },
            //...
            "resources": [
                {
                    "type": "config",
                    "name": "appsettings",
                    //...
                    "dependsOn": [
                        "[resourceId('Microsoft.Web/sites',
variables('functionAppName'))]",
                        "[resourceId('Microsoft.KeyVault/vaults/',
variables('keyVaultName'))]",
                        "[resourceId('Microsoft.KeyVault/vaults/secrets',
variables('keyVaultName'), variables('storageConnectionStringName'))]",
                        "[resourceId('Microsoft.KeyVault/vaults/secrets',
variables('keyVaultName'), variables('appInsightsKeyName'))]"
                    ],
                    "properties": {
                        "AzureWebJobsStorage":
"[concat('@Microsoft.KeyVault(SecretUri=',
reference(variables('storageConnectionStringResourceId')).secretUriWithVersio
n, ')')]",
                        "WEBSITE_CONTENTAZUREFILECONNECTIONSTRING":
"[concat('@Microsoft.KeyVault(SecretUri=',
reference(variables('storageConnectionStringResourceId')).secretUriWithVersio
n, ')')]",
                        "APPINSIGHTS_INSTRUMENTATIONKEY":
"[concat('@Microsoft.KeyVault(SecretUri=',
reference(variables('appInsightsKeyResourceId')).secretUriWithVersion,
')')]",
                        "WEBSITE_ENABLE_SYNC_UPDATE_SITE": "true"
                        //...
                    }
                },
                {
                    "type": "sourcecontrols",
                    "name": "web",
                    //...
                    "dependsOn": [
                        "[resourceId('Microsoft.Web/sites',
variables('functionAppName'))]",
                        "[resourceId('Microsoft.Web/sites/config',
variables('functionAppName'), 'appsettings')]"
                    ],
                }
            ]
        },
        {
            "type": "Microsoft.KeyVault/vaults",
            "name": "[variables('keyVaultName')]",
            //...
            "dependsOn": [
                "[resourceId('Microsoft.Web/sites',
variables('functionAppName'))]"
            ],
            "properties": {
                //...
                "accessPolicies": [
                    {
                        "tenantId":
"[reference(concat('Microsoft.Web/sites/',  variables('functionAppName'),
'/providers/Microsoft.ManagedIdentity/Identities/default'), '2015-08-31-
PREVIEW').tenantId]",
                        "objectId":
"[reference(concat('Microsoft.Web/sites/',  variables('functionAppName'),
'/providers/Microsoft.ManagedIdentity/Identities/default'), '2015-08-31-
PREVIEW').principalId]",
                        "permissions": {
                            "secrets": [ "get" ]
                        }
                    }
                ]
            },
            "resources": [
                {
                    "type": "secrets",
                    "name": "[variables('storageConnectionStringName')]",
                    //...
                    "dependsOn": [
                        "[resourceId('Microsoft.KeyVault/vaults/',
variables('keyVaultName'))]",
                        "[resourceId('Microsoft.Storage/storageAccounts',
variables('storageAccountName'))]"
                    ],
                    "properties": {
                        "value":
"[concat('DefaultEndpointsProtocol=https;AccountName=',
variables('storageAccountName'), ';AccountKey=',
listKeys(variables('storageAccountResourceId'),'2015-05-01-preview').key1)]"
                    }
                },
                {
                    "type": "secrets",
                    "name": "[variables('appInsightsKeyName')]",
                    //...
                    "dependsOn": [
                        "[resourceId('Microsoft.KeyVault/vaults/',
variables('keyVaultName'))]",
                        "[resourceId('Microsoft.Insights/components',
variables('appInsightsName'))]"
                    ],
                    "properties": {
                        "value":
"[reference(resourceId('microsoft.insights/components/',
variables('appInsightsName')), '2015-05-01').InstrumentationKey]"
                    }
                }
            ]
        }
    ]
}
```

Default Value:

By default, no Azure Key Vaults are created.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-identity-management#im-3-manage-application-identities-securely-and-automatically
3. https://docs.microsoft.com/en-us/cli/azure/keyvault?view=azure-cli-latest
4. https://docs.microsoft.com/en-us/cli/azure/keyvault?view=azure-cli-latest

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.1 Establish and Maintain a Data Management Process Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	13.1 Maintain an Inventory Sensitive Information Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.	●	●	●

9.12 Ensure that 'Remote debugging' is set to 'Off' (Automated)

Profile Applicability:

- Level 1

Description:

Remote Debugging allows Azure App Service to be debugged in real-time directly on the Azure environment. When remote debugging is enabled, it opens a communication channel that could potentially be exploited by unauthorized users if not properly secured.

Rationale:

Disabling remote debugging on Azure App Service is primarily about enhancing security.

Remote debugging opens a communication channel that can be exploited by attackers. By disabling it, you reduce the number of potential entry points for unauthorized access.

If remote debugging is enabled without proper access controls, it can allow unauthorized users to connect to your application, potentially leading to data breaches or malicious code execution.

During a remote debugging session, sensitive information might be exposed. Disabling remote debugging helps ensure that such data remains secure. This minimizes the use of remote access tools to reduce risk.

Impact:

You will not be able to connect to your application from a remote location to diagnose and fix issues in real-time. You will not be able to step through code, set breakpoints, or inspect variables and the call stack while the application is running on the server. Remote debugging is particularly useful for diagnosing issues that only occur in the production environment. Without it, you will need to rely on logs and other diagnostic tools.

Audit:

Audit from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under `Setting` section, Click on `Configuration`
5. Under the `General settings` tab, check the `Remote debugging` option. Ensure it is set to `Off`.

Audit from Azure CLI
To check remote debugging status for an existing app, run the following command,

```
az webapp config show --resource-group <resource_group_name> --name
<app_name> --query remoteDebuggingEnabled
```

The output should be `false` if remote debugging is disabled.

Audit from PowerShell
To check remote debugging status for an existing app, run the following command,

```
Get-AzWebApp -ResourceGroupName <resource_group_name> -Name <app_name>
|Select-Object -ExpandProperty SiteConfig
```

The output of `remoteDebuggingEnabled` should be `false` if remote debugging is disabled.

Audit from Azure Policy
If referencing a digital copy of this Benchmark, clicking a Policy ID will open a link to the associated Policy definition in Azure.
If referencing a printed copy, you can search Policy IDs from this URL:
https://portal.azure.com/#view/Microsoft_Azure_Policy/PolicyMenuBlade/~/Definitions

- **Policy ID:** cb510bfd-1cba-4d9f-a230-cb0976f4bb71 **- Name:** 'App Service apps should have remote debugging turned off'
- **Policy ID:** 25a5046c-c423-4805-9235-e844ae9ef49b **- Name:** 'Configure Function apps to turn off remote debugging'

Remediation:

Remediate from Azure Portal

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under `Setting` section, Click on `Configuration`
5. Under the `General settings` tab, set the `Remote debugging` option to `Off`.

Remediate from Azure CLI
To set remote debugging status to off, run the following command

```
az webapp config set --resource-group <resource_group_name> --name <app_name>
--remote-debugging-enabled false
```

Remediation from PowerShell
To set remote debugging status to off, run the following command

```
Set-AzWebApp -ResourceGroupName <resource_group_name> -Name <app_name> -
RemoteDebuggingEnabled $false
```

Default Value:

By default, remote debugging is set to `off`

References:

1. https://learn.microsoft.com/en-us/visualstudio/debugger/remote-debugging-azure-app-service?view=vs-2022
2. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-posture-vulnerability-management#pv-2-audit-and-enforce-secure-configurations

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	12.3 Securely Manage Network Infrastructure Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS.		●	●
v7	9.2 Ensure Only Approved Ports, Protocols and Services Are Running Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

10 Miscellaneous

10.1 Ensure that Resource Locks are set for Mission-Critical Azure Resources (Manual)

Profile Applicability:

- Level 2

Description:

Resource Manager Locks provide a way for administrators to lock down Azure resources to prevent deletion of, or modifications to, a resource. These locks sit outside of the Role Based Access Controls (RBAC) hierarchy and, when applied, will place restrictions on the resource for all users. These locks are very useful when there is an important resource in a subscription that users should not be able to delete or change. Locks can help prevent accidental and malicious changes or deletion.

Rationale:

As an administrator, it may be necessary to lock a subscription, resource group, or resource to prevent other users in the organization from accidentally deleting or modifying critical resources. The lock level can be set to to `CanNotDelete` or `ReadOnly` to achieve this purpose.

- `CanNotDelete` means authorized users can still read and modify a resource, but they cannot delete the resource.
- `ReadOnly` means authorized users can read a resource, but they cannot delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Impact:

There can be unintended outcomes of locking a resource. Applying a lock to a parent service will cause it to be inherited by all resources within. Conversely, applying a lock to a resource may not apply to connected storage, leaving it unlocked. Please see the documentation for further information.

Audit:

Audit from Azure Portal

1. Navigate to the specific Azure Resource or Resource Group.
2. Click on `Locks`.
3. Ensure the lock is defined with name and description, with type `Read-only` or `Delete` as appropriate.

Audit from Azure CLI

Review the list of all locks set currently:

```
az lock list --resource-group <resourcegroupname> --resource-name
<resourcename> --namespace <Namespace> --resource-type <type> --parent ""
```

Audit from PowerShell

Run the following command to list all resources.

```
Get-AzResource
```

For each resource, run the following command to check for Resource Locks.

```
Get-AzResourceLock -ResourceName <Resource Name> -ResourceType <Resource
Type> -ResourceGroupName <Resource Group Name>
```

Review the output of the `Properties` setting. Compliant settings will have the `CanNotDelete` or `ReadOnly` value.

Remediation:

Remediate from Azure Portal

1. Navigate to the specific Azure Resource or Resource Group.
2. For each mission critical resource, click on `Locks`.
3. Click `Add`.
4. Give the lock a name and a description, then select the type, `Read-only` or `Delete` as appropriate.
5. Click OK.

Remediate from Azure CLI

To lock a resource, provide the name of the resource, its resource type, and its resource group name.

```
az lock create --name <LockName> --lock-type <CanNotDelete/Read-only> --
resource-group <resourceGroupName> --resource-name <resourceName> --resource-
type <resourceType>
```

Remediate from PowerShell

```
Get-AzResourceLock -ResourceName <Resource Name> -ResourceType <Resource
Type> -ResourceGroupName <Resource Group Name> -Locktype <CanNotDelete/Read-
only>
```

Default Value:

By default, no locks are set.

References:

1. https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources
2. https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-subscription-governance#azure-resource-locks
3. https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking
4. https://learn.microsoft.com/en-us/security/benchmark/azure/mcsb-asset-management#am-4-limit-access-to-asset-management

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	3.3 Configure Data Access Control Lists Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v7	14.6 Protect Information through Access Control Lists Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1	**Introduction**		
1.1	**CIS Microsoft Azure Foundations Benchmarks**		
1.2	**CIS Microsoft Azure Service Category Benchmarks**		
1.3	**Multiple Methods of Audit and Remediation**		
2	**Identity**		
2.1	**Security Defaults (Per-User MFA)**		
2.1.1	Ensure Security Defaults is enabled on Microsoft Entra ID (Manual)	□	□
2.1.2	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users (Manual)	□	□
2.1.3	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users (Manual)	□	□
2.1.4	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled (Manual)	□	□
2.2	**Conditional Access**		
2.2.1	Ensure Trusted Locations Are Defined (Manual)	□	□
2.2.2	Ensure that an exclusionary Geographic Access Policy is considered (Manual)	□	□
2.2.3	Ensure that an exclusionary Device code flow policy is considered (Manual)	□	□
2.2.4	Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups (Manual)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.2.5	Ensure that A Multi-factor Authentication Policy Exists for All Users (Manual)	□	□
2.2.6	Ensure Multi-factor Authentication is Required for Risky Sign-ins (Manual)	□	□
2.2.7	Ensure Multi-factor Authentication is Required for Windows Azure Service Management API (Manual)	□	□
2.2.8	Ensure Multi-factor Authentication is Required to access Microsoft Admin Portals (Manual)	□	□
2.3	Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes' (Automated)	□	□
2.4	Ensure Guest Users Are Reviewed on a Regular Basis (Manual)	□	□
2.5	Ensure That 'Number of methods required to reset' is set to '2' (Manual)	□	□
2.6	Ensure that account 'Lockout Threshold' is less than or equal to '10' (Manual)	□	□
2.7	Ensure that account 'Lockout duration in seconds' is greater than or equal to '60' (Manual)	□	□
2.8	Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization (Manual)	□	□
2.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0' (Manual)	□	□
2.10	Ensure that 'Notify users on password resets?' is set to 'Yes' (Manual)	□	□
2.11	Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes' (Manual)	□	□
2.12	Ensure `User consent for applications` is set to `Do not allow user consent` (Manual)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.13	Ensure ‘User consent for applications’ Is Set To ‘Allow for Verified Publishers’ (Manual)	□	□
2.14	Ensure That ‘Users Can Register Applications’ Is Set to ‘No’ (Automated)	□	□
2.15	Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' (Automated)	□	□
2.16	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users' (Automated)	□	□
2.17	Ensure That 'Restrict access to Microsoft Entra admin center' is Set to 'Yes' (Manual)	□	□
2.18	Ensure that 'Restrict user ability to access groups features in the Access Pane' is Set to 'Yes' (Manual)	□	□
2.19	Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No' (Manual)	□	□
2.20	Ensure that 'Owners can manage group membership requests in My Groups' is set to 'No' (Manual)	□	□
2.21	Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No' (Manual)	□	□
2.22	Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes' (Manual)	□	□
2.23	Ensure That No Custom Subscription Administrator Roles Exist (Automated)	□	□
2.24	Ensure a Custom Role is Assigned Permissions for Administering Resource Locks (Manual)	□	□
2.25	Ensure That 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' Is Set To 'Permit no one' (Manual)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.26	Ensure fewer than 5 users have global administrator assignment (Manual)	□	□
3	**Security**		
3.1	**Microsoft Defender for Cloud**		
3.1.1	**Microsoft Cloud Security Posture Management (CSPM)**		
3.1.1.1	Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On' (Automated)	□	□
3.1.1.2	Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected (Automated)	□	□
3.1.2	**Defender Plan: APIs**		
3.1.3	**Defender Plan: Servers**		
3.1.3.1	Ensure That Microsoft Defender for Servers Is Set to 'On' (Automated)	□	□
3.1.3.2	Ensure that 'Vulnerability assessment for machines' component status is set to 'On' (Manual)	□	□
3.1.3.3	Ensure that 'Endpoint protection' component status is set to 'On' (Manual)	□	□
3.1.3.4	Ensure that 'Agentless scanning for machines' component status is set to 'On' (Manual)	□	□
3.1.3.5	Ensure that 'File Integrity Monitoring' component status is set to 'On' (Manual)	□	□
3.1.4	**Defender Plan: Containers**		
3.1.4.1	Ensure That Microsoft Defender for Containers Is Set To 'On' (Automated)	□	□
3.1.4.2	Ensure that 'Agentless discovery for Kubernetes' component status 'On' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.4.3	Ensure that 'Agentless container vulnerability assessment' component status is 'On' (Automated)	□	□
3.1.5	**Defender Plan: Storage**		
3.1.5.1	Ensure That Microsoft Defender for Storage Is Set To 'On' (Automated)	□	□
3.1.6	**Defender Plan: App Service**		
3.1.6.1	Ensure That Microsoft Defender for App Services Is Set To 'On' (Automated)	□	□
3.1.7	**Defender Plan: Databases**		
3.1.7.1	Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On' (Automated)	□	□
3.1.7.2	Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On' (Automated)	□	□
3.1.7.3	Ensure That Microsoft Defender for (Managed Instance) Azure SQL Databases Is Set To 'On' (Automated)	□	□
3.1.7.4	Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On' (Automated)	□	□
3.1.8	**Defender Plan: Key Vault**		
3.1.8.1	Ensure That Microsoft Defender for Key Vault Is Set To 'On' (Automated)	□	□
3.1.9	**Defender Plan: Resource Manager**		
3.1.9.1	Ensure That Microsoft Defender for Resource Manager Is Set To 'On' (Automated)	□	□
3.1.10	Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled' (Manual)	□	□
3.1.12	Ensure That 'All users with the following roles' is set to 'Owner' (Automated)	□	□
3.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email (Automated)	□	□
3.1.14	Ensure That 'Notify about alerts with the following severity' is Set to 'High' (Automated)	□	□
3.1.15	Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled (Manual)	□	□
3.1.16	[LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On' (Automated)	□	□
3.2	**Microsoft Defender for IoT**		
3.2.1	Ensure That Microsoft Defender for IoT Hub Is Set To 'On' (Manual)	□	□
3.3	**Key Vault**		
3.3.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults (Automated)	□	□
3.3.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults. (Automated)	□	□
3.3.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults (Automated)	□	□
3.3.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults (Automated)	□	□
3.3.5	Ensure the Key Vault is Recoverable (Automated)	□	□
3.3.6	Enable Role Based Access Control for Azure Key Vault (Automated)	□	□

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
3.3.7	Ensure that Private Endpoints are Used for Azure Key Vault (Automated)	□	□
3.3.8	Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services (Automated)	□	□
4	**Storage Accounts**		
4.1	Ensure that 'Secure transfer required' is set to 'Enabled' (Automated)	□	□
4.2	Ensure that ‘Enable Infrastructure Encryption’ for Each Storage Account in Azure Storage is Set to ‘enabled’ (Automated)	□	□
4.3	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account (Manual)	□	□
4.4	Ensure that Storage Account Access Keys are Periodically Regenerated (Manual)	□	□
4.5	Ensure that Shared Access Signature Tokens Expire Within an Hour (Manual)	□	□
4.6	Ensure that 'Public Network Access' is 'Disabled' for storage accounts (Automated)	□	□
4.7	Ensure Default Network Access Rule for Storage Accounts is Set to Deny (Automated)	□	□
4.8	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access (Automated)	□	□
4.9	Ensure Private Endpoints are used to access Storage Accounts (Automated)	□	□
4.10	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage (Automated)	□	□
4.11	Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK) (Manual)	□	□

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
4.12	Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests (Automated)	□	□
4.13	Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests (Automated)	□	□
4.14	Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests (Automated)	□	□
4.15	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2' (Automated)	□	□
4.16	Ensure 'Cross Tenant Replication' is not enabled (Automated)	□	□
4.17	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled' (Automated)	□	□
5	**Database Services**		
5.1	**Azure SQL Database**		
5.1.1	Ensure that 'Auditing' is set to 'On' (Automated)	□	□
5.1.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) (Automated)	□	□
5.1.3	Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key (Automated)	□	□
5.1.4	Ensure that Microsoft Entra authentication is Configured for SQL Servers (Automated)	□	□
5.1.5	Ensure that 'Data encryption' is set to 'On' on a SQL Database (Automated)	□	□
5.1.6	Ensure that 'Auditing' Retention is 'greater than 90 days' (Automated)	□	□
5.1.7	Ensure Public Network Access is Disabled (Manual)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2	**Azure Database for PostgreSQL**		
5.2.1	Ensure server parameter 'require_secure_transport' is set to 'ON' for PostgreSQL flexible server (Automated)	□	□
5.2.2	Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL flexible server (Automated)	□	□
5.2.3	Ensure server parameter 'connection_throttle.enable' is set to 'ON' for PostgreSQL flexible server (Automated)	□	□
5.2.4	Ensure server parameter 'logfiles.retention_days' is greater than 3 days for PostgreSQL flexible server (Automated)	□	□
5.2.5	Ensure 'Allow public access from any Azure service within Azure to this server' for PostgreSQL flexible server is disabled (Automated)	□	□
5.2.6	[LEGACY] Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL single server (Automated)	□	□
5.2.7	[LEGACY] Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL single server (Automated)	□	□
5.2.8	[LEGACY] Ensure 'Infrastructure double encryption' for PostgreSQL single server is 'Enabled' (Automated)	□	□
5.3	**Azure Database for MySQL**		
5.3.1	Ensure server parameter 'require_secure_transport' is set to 'ON' for MySQL flexible server (Automated)	□	□
5.3.2	Ensure server parameter 'tls_version' is set to 'TLSv1.2' (or higher) for MySQL flexible server (Automated)	□	□
5.3.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL flexible server (Automated)	□	□
5.3.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL flexible server (Automated)	□	□

CIS Benchmark Recommendation		**Set Correctly**	
		Yes	No
5.4	**Azure Cosmos DB**		
5.4.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks (Automated)	□	□
5.4.2	Ensure That Private Endpoints Are Used Where Possible (Automated)	□	□
5.4.3	Use Entra ID Client Authentication and Azure RBAC where possible (Manual)	□	□
6	**Logging and Monitoring**		
6.1	**Configuring Diagnostic Settings**		
6.1.1	Ensure that a 'Diagnostic Setting' exists for Subscription Activity Logs (Manual)	□	□
6.1.2	Ensure Diagnostic Setting captures appropriate categories (Automated)	□	□
6.1.3	Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (CMK) (Automated)	□	□
6.1.4	Ensure that logging for Azure Key Vault is 'Enabled' (Automated)	□	□
6.1.5	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics (Manual)	□	□
6.1.6	Ensure that logging for Azure AppService 'HTTP logs' is enabled (Manual)	□	□
6.2	**Monitoring using Activity Log Alerts**		
6.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment (Automated)	□	□
6.2.2	Ensure that Activity Log Alert exists for Delete Policy Assignment (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.2.3	Ensure that Activity Log Alert exists for Create or Update Network Security Group (Automated)	□	□
6.2.4	Ensure that Activity Log Alert exists for Delete Network Security Group (Automated)	□	□
6.2.5	Ensure that Activity Log Alert exists for Create or Update Security Solution (Automated)	□	□
6.2.6	Ensure that Activity Log Alert exists for Delete Security Solution (Automated)	□	□
6.2.7	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule (Automated)	□	□
6.2.8	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule (Automated)	□	□
6.2.9	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule (Automated)	□	□
6.2.10	Ensure that Activity Log Alert exists for Delete Public IP Address rule (Automated)	□	□
6.3	**Configuring Application Insights**		
6.3.1	Ensure Application Insights are Configured (Automated)	□	□
6.4	Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it (Manual)	□	□
6.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) (Manual)	□	□
7	**Networking**		
7.1	Ensure that RDP access from the Internet is evaluated and restricted (Automated)	□	□
7.2	Ensure that SSH access from the Internet is evaluated and restricted (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
7.3	Ensure that UDP access from the Internet is evaluated and restricted (Automated)	□	□
7.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted (Automated)	□	□
7.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' (Automated)	□	□
7.6	Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use (Automated)	□	□
7.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis (Manual)	□	□
8	**Virtual Machines**		
8.1	Ensure an Azure Bastion Host Exists (Automated)	□	□
8.2	Ensure Virtual Machines are utilizing Managed Disks (Automated)	□	□
8.3	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK) (Automated)	□	□
8.4	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK) (Automated)	□	□
8.5	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks' (Automated)	□	□
8.6	Ensure that 'Enable Data Access Authentication Mode' is 'Checked' (Automated)	□	□
8.7	Ensure that Only Approved Extensions Are Installed (Manual)	□	□
8.8	Ensure that Endpoint Protection for all Virtual Machines is installed (Manual)	□	□
8.9	[Legacy] Ensure that VHDs are Encrypted (Manual)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
8.10	Ensure only MFA enabled identities can access privileged Virtual Machine (Manual)	□	□
8.11	Ensure Trusted Launch is enabled on Virtual Machines (Automated)	□	□
9	**AppService**		
9.1	Ensure 'HTTPS Only' is set to `On` (Automated)	□	□
9.2	Ensure App Service Authentication is set up for apps in Azure App Service (Automated)	□	□
9.3	Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled' (Automated)	□	□
9.4	Ensure Web App is using the latest version of TLS encryption (Automated)	□	□
9.5	Ensure that Register with Entra ID is enabled on App Service (Automated)	□	□
9.6	Ensure that 'Basic Authentication' is 'Disabled' (Manual)	□	□
9.7	Ensure that 'PHP version' is currently supported (if in use) (Manual)	□	□
9.8	Ensure that 'Python version' is currently supported (if in use) (Manual)	□	□
9.9	Ensure that 'Java version' is currently supported (if in use) (Manual)	□	□
9.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use) (Automated)	□	□
9.11	Ensure Azure Key Vaults are Used to Store Secrets (Manual)	□	□
9.12	Ensure that 'Remote debugging' is set to 'Off' (Automated)	□	□

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
10	**Miscellaneous**		
10.1	Ensure that Resource Locks are set for Mission-Critical Azure Resources (Manual)	□	□

Appendix: CIS Controls v7 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure Security Defaults is enabled on Microsoft Entra ID	□	□
2.2.2	Ensure that an exclusionary Geographic Access Policy is considered	□	□
2.2.3	Ensure that an exclusionary Device code flow policy is considered	□	□
2.3	Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes'	□	□
2.4	Ensure Guest Users Are Reviewed on a Regular Basis	□	□
2.12	Ensure `User consent for applications` is set to `Do not allow user consent`	□	□
2.13	Ensure ‘User consent for applications’ Is Set To ‘Allow for Verified Publishers’	□	□
2.14	Ensure That ‘Users Can Register Applications’ Is Set to ‘No’	□	□
2.15	Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	□	□
2.17	Ensure That 'Restrict access to Microsoft Entra admin center' is Set to 'Yes'	□	□
2.18	Ensure that 'Restrict user ability to access groups features in the Access Pane' is Set to 'Yes'	□	□
2.19	Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'	□	□
2.20	Ensure that 'Owners can manage group membership requests in My Groups' is set to 'No'	□	□
2.21	Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'	□	□
2.24	Ensure a Custom Role is Assigned Permissions for Administering Resource Locks	□	□

Recommendation		Set Correctly	
		Yes	No
2.25	Ensure That 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' Is Set To 'Permit no one'	□	□
3.1.10	Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed'	□	□
3.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'	□	□
3.1.12	Ensure That 'All users with the following roles' is set to 'Owner'	□	□
3.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email	□	□
3.3.5	Ensure the Key Vault is Recoverable	□	□
3.3.6	Enable Role Based Access Control for Azure Key Vault	□	□
4.6	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	□	□
4.10	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	□	□
4.17	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	□	□
5.1.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	□	□
5.1.7	Ensure Public Network Access is Disabled	□	□
5.2.2	Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.3	Ensure server parameter 'connection_throttle.enable' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.5	Ensure 'Allow public access from any Azure service within Azure to this server' for PostgreSQL flexible server is disabled	□	□
5.2.6	[LEGACY] Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL single server	□	□
5.2.7	[LEGACY] Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL single server	□	□
5.3.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL flexible server	□	□

Recommendation		Set Correctly	
		Yes	No
5.3.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL flexible server	□	□
5.4.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	□	□
6.3.1	Ensure Application Insights are Configured	□	□
6.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)	□	□
7.6	Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use	□	□
7.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis	□	□
8.1	Ensure an Azure Bastion Host Exists	□	□
8.5	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks'	□	□
8.6	Ensure that 'Enable Data Access Authentication Mode' is 'Checked'	□	□
8.7	Ensure that Only Approved Extensions Are Installed	□	□
8.8	Ensure that Endpoint Protection for all Virtual Machines is installed	□	□
8.11	Ensure Trusted Launch is enabled on Virtual Machines	□	□
9.2	Ensure App Service Authentication is set up for apps in Azure App Service	□	□
9.7	Ensure that 'PHP version' is currently supported (if in use)	□	□
9.8	Ensure that 'Python version' is currently supported (if in use)	□	□
9.9	Ensure that 'Java version' is currently supported (if in use)	□	□
9.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use)	□	□
9.11	Ensure Azure Key Vaults are Used to Store Secrets	□	□
10.1	Ensure that Resource Locks are set for Mission-Critical Azure Resources	□	□

Appendix: CIS Controls v7 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure Security Defaults is enabled on Microsoft Entra ID	□	□
2.1.2	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users	□	□
2.1.3	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users	□	□
2.1.4	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled	□	□
2.2.1	Ensure Trusted Locations Are Defined	□	□
2.2.2	Ensure that an exclusionary Geographic Access Policy is considered	□	□
2.2.3	Ensure that an exclusionary Device code flow policy is considered	□	□
2.2.4	Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups	□	□
2.2.5	Ensure that A Multi-factor Authentication Policy Exists for All Users	□	□
2.2.6	Ensure Multi-factor Authentication is Required for Risky Sign-ins	□	□
2.2.7	Ensure Multi-factor Authentication is Required for Windows Azure Service Management API	□	□
2.2.8	Ensure Multi-factor Authentication is Required to access Microsoft Admin Portals	□	□
2.3	Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes'	□	□
2.4	Ensure Guest Users Are Reviewed on a Regular Basis	□	□
2.5	Ensure That 'Number of methods required to reset' is set to '2'	□	□
2.8	Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization	□	□

Recommendation		Set Correctly	
		Yes	No
2.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	□	□
2.10	Ensure that 'Notify users on password resets?' is set to 'Yes'	□	□
2.11	Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes'	□	□
2.12	Ensure `User consent for applications` is set to `Do not allow user consent`	□	□
2.13	Ensure 'User consent for applications' Is Set To 'Allow for Verified Publishers'	□	□
2.14	Ensure That 'Users Can Register Applications' Is Set to 'No'	□	□
2.15	Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	□	□
2.16	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'	□	□
2.17	Ensure That 'Restrict access to Microsoft Entra admin center' is Set to 'Yes'	□	□
2.18	Ensure that 'Restrict user ability to access groups features in the Access Pane' is Set to 'Yes'	□	□
2.19	Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'	□	□
2.20	Ensure that 'Owners can manage group membership requests in My Groups' is set to 'No'	□	□
2.21	Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'	□	□
2.22	Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes'	□	□
2.23	Ensure That No Custom Subscription Administrator Roles Exist	□	□
2.24	Ensure a Custom Role is Assigned Permissions for Administering Resource Locks	□	□
2.25	Ensure That 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' Is Set To 'Permit no one'	□	□

Recommendation		Set Correctly	
		Yes	No
2.26	Ensure fewer than 5 users have global administrator assignment	□	□
3.1.1.1	Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On'	□	□
3.1.1.2	Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected	□	□
3.1.3.1	Ensure That Microsoft Defender for Servers Is Set to 'On'	□	□
3.1.3.2	Ensure that 'Vulnerability assessment for machines' component status is set to 'On'	□	□
3.1.3.3	Ensure that 'Endpoint protection' component status is set to 'On'	□	□
3.1.3.4	Ensure that 'Agentless scanning for machines' component status is set to 'On'	□	□
3.1.3.5	Ensure that 'File Integrity Monitoring' component status is set to 'On'	□	□
3.1.4.1	Ensure That Microsoft Defender for Containers Is Set To 'On'	□	□
3.1.4.2	Ensure that 'Agentless discovery for Kubernetes' component status 'On'	□	□
3.1.4.3	Ensure that 'Agentless container vulnerability assessment' component status is 'On'	□	□
3.1.5.1	Ensure That Microsoft Defender for Storage Is Set To 'On'	□	□
3.1.6.1	Ensure That Microsoft Defender for App Services Is Set To 'On'	□	□
3.1.7.1	Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On'	□	□
3.1.7.2	Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On'	□	□
3.1.7.3	Ensure That Microsoft Defender for (Managed Instance) Azure SQL Databases Is Set To 'On'	□	□
3.1.7.4	Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On'	□	□
3.1.8.1	Ensure That Microsoft Defender for Key Vault Is Set To 'On'	□	□

Recommendation		Set Correctly	
		Yes	No
3.1.9.1	Ensure That Microsoft Defender for Resource Manager Is Set To 'On'	□	□
3.1.10	Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed'	□	□
3.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'	□	□
3.1.12	Ensure That 'All users with the following roles' is set to 'Owner'	□	□
3.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email	□	□
3.1.15	Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled	□	□
3.1.16	[LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On'	□	□
3.2.1	Ensure That Microsoft Defender for IoT Hub Is Set To 'On'	□	□
3.3.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults	□	□
3.3.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults.	□	□
3.3.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	□	□
3.3.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults	□	□
3.3.5	Ensure the Key Vault is Recoverable	□	□
3.3.6	Enable Role Based Access Control for Azure Key Vault	□	□
3.3.7	Ensure that Private Endpoints are Used for Azure Key Vault	□	□
3.3.8	Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services	□	□
4.1	Ensure that 'Secure transfer required' is set to 'Enabled'	□	□
4.3	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	□	□
4.4	Ensure that Storage Account Access Keys are Periodically Regenerated	□	□

Recommendation		Set Correctly	
		Yes	No
4.5	Ensure that Shared Access Signature Tokens Expire Within an Hour	□	□
4.6	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	□	□
4.9	Ensure Private Endpoints are used to access Storage Accounts	□	□
4.10	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	□	□
4.12	Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests	□	□
4.13	Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests	□	□
4.14	Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests	□	□
4.15	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	□	□
4.16	Ensure 'Cross Tenant Replication' is not enabled	□	□
4.17	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	□	□
5.1.1	Ensure that 'Auditing' is set to 'On'	□	□
5.1.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	□	□
5.1.3	Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key	□	□
5.1.4	Ensure that Microsoft Entra authentication is Configured for SQL Servers	□	□
5.1.6	Ensure that 'Auditing' Retention is 'greater than 90 days'	□	□
5.1.7	Ensure Public Network Access is Disabled	□	□
5.2.1	Ensure server parameter 'require_secure_transport' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.2	Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.3	Ensure server parameter 'connection_throttle.enable' is set to 'ON' for PostgreSQL flexible server	□	□

Recommendation		Set Correctly	
		Yes	No
5.2.4	Ensure server parameter 'logfiles.retention_days' is greater than 3 days for PostgreSQL flexible server	□	□
5.2.5	Ensure 'Allow public access from any Azure service within Azure to this server' for PostgreSQL flexible server is disabled	□	□
5.2.6	[LEGACY] Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL single server	□	□
5.2.7	[LEGACY] Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL single server	□	□
5.3.1	Ensure server parameter 'require_secure_transport' is set to 'ON' for MySQL flexible server	□	□
5.3.2	Ensure server parameter 'tls_version' is set to 'TLSv1.2' (or higher) for MySQL flexible server	□	□
5.3.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL flexible server	□	□
5.3.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL flexible server	□	□
5.4.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	□	□
5.4.2	Ensure That Private Endpoints Are Used Where Possible	□	□
5.4.3	Use Entra ID Client Authentication and Azure RBAC where possible	□	□
6.1.1	Ensure that a 'Diagnostic Setting' exists for Subscription Activity Logs	□	□
6.1.2	Ensure Diagnostic Setting captures appropriate categories	□	□
6.1.4	Ensure that logging for Azure Key Vault is 'Enabled'	□	□
6.1.5	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics	□	□
6.1.6	Ensure that logging for Azure AppService 'HTTP logs' is enabled	□	□
6.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment	□	□
6.2.2	Ensure that Activity Log Alert exists for Delete Policy Assignment	□	□

Recommendation		Set Correctly	
		Yes	No
6.2.3	Ensure that Activity Log Alert exists for Create or Update Network Security Group	□	□
6.2.4	Ensure that Activity Log Alert exists for Delete Network Security Group	□	□
6.2.5	Ensure that Activity Log Alert exists for Create or Update Security Solution	□	□
6.2.6	Ensure that Activity Log Alert exists for Delete Security Solution	□	□
6.2.7	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule	□	□
6.2.8	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule	□	□
6.2.9	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule	□	□
6.2.10	Ensure that Activity Log Alert exists for Delete Public IP Address rule	□	□
6.3.1	Ensure Application Insights are Configured	□	□
6.4	Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it	□	□
6.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)	□	□
7.1	Ensure that RDP access from the Internet is evaluated and restricted	□	□
7.2	Ensure that SSH access from the Internet is evaluated and restricted	□	□
7.3	Ensure that UDP access from the Internet is evaluated and restricted	□	□
7.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted	□	□
7.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'	□	□
7.6	Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use	□	□
7.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis	□	□

Recommendation		Set Correctly	
		Yes	No
8.1	Ensure an Azure Bastion Host Exists	□	□
8.5	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks'	□	□
8.6	Ensure that 'Enable Data Access Authentication Mode' is 'Checked'	□	□
8.7	Ensure that Only Approved Extensions Are Installed	□	□
8.8	Ensure that Endpoint Protection for all Virtual Machines is installed	□	□
8.10	Ensure only MFA enabled identities can access privileged Virtual Machine	□	□
8.11	Ensure Trusted Launch is enabled on Virtual Machines	□	□
9.1	Ensure 'HTTPS Only' is set to \`On\`	□	□
9.2	Ensure App Service Authentication is set up for apps in Azure App Service	□	□
9.3	Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled'	□	□
9.4	Ensure Web App is using the latest version of TLS encryption	□	□
9.5	Ensure that Register with Entra ID is enabled on App Service	□	□
9.6	Ensure that 'Basic Authentication' is 'Disabled'	□	□
9.7	Ensure that 'PHP version' is currently supported (if in use)	□	□
9.8	Ensure that 'Python version' is currently supported (if in use)	□	□
9.9	Ensure that 'Java version' is currently supported (if in use)	□	□
9.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use)	□	□
9.11	Ensure Azure Key Vaults are Used to Store Secrets	□	□
9.12	Ensure that 'Remote debugging' is set to 'Off'	□	□
10.1	Ensure that Resource Locks are set for Mission-Critical Azure Resources	□	□

Appendix: CIS Controls v7 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure Security Defaults is enabled on Microsoft Entra ID	□	□
2.1.2	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users	□	□
2.1.3	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users	□	□
2.1.4	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled	□	□
2.2.1	Ensure Trusted Locations Are Defined	□	□
2.2.2	Ensure that an exclusionary Geographic Access Policy is considered	□	□
2.2.3	Ensure that an exclusionary Device code flow policy is considered	□	□
2.2.4	Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups	□	□
2.2.5	Ensure that A Multi-factor Authentication Policy Exists for All Users	□	□
2.2.6	Ensure Multi-factor Authentication is Required for Risky Sign-ins	□	□
2.2.7	Ensure Multi-factor Authentication is Required for Windows Azure Service Management API	□	□
2.2.8	Ensure Multi-factor Authentication is Required to access Microsoft Admin Portals	□	□
2.3	Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes'	□	□
2.4	Ensure Guest Users Are Reviewed on a Regular Basis	□	□
2.5	Ensure That 'Number of methods required to reset' is set to '2'	□	□
2.8	Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization	□	□

Recommendation		Set Correctly	
		Yes	No
2.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	□	□
2.10	Ensure that 'Notify users on password resets?' is set to 'Yes'	□	□
2.11	Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes'	□	□
2.12	Ensure `User consent for applications` is set to `Do not allow user consent`	□	□
2.13	Ensure ‘User consent for applications’ Is Set To ‘Allow for Verified Publishers’	□	□
2.14	Ensure That ‘Users Can Register Applications’ Is Set to ‘No’	□	□
2.15	Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	□	□
2.16	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'	□	□
2.17	Ensure That 'Restrict access to Microsoft Entra admin center' is Set to 'Yes'	□	□
2.18	Ensure that 'Restrict user ability to access groups features in the Access Pane' is Set to 'Yes'	□	□
2.19	Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'	□	□
2.20	Ensure that 'Owners can manage group membership requests in My Groups' is set to 'No'	□	□
2.21	Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'	□	□
2.22	Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes'	□	□
2.23	Ensure That No Custom Subscription Administrator Roles Exist	□	□
2.24	Ensure a Custom Role is Assigned Permissions for Administering Resource Locks	□	□
2.25	Ensure That 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' Is Set To 'Permit no one'	□	□

Recommendation		Set Correctly	
		Yes	No
2.26	Ensure fewer than 5 users have global administrator assignment	□	□
3.1.1.1	Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On'	□	□
3.1.1.2	Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected	□	□
3.1.3.1	Ensure That Microsoft Defender for Servers Is Set to 'On'	□	□
3.1.3.2	Ensure that 'Vulnerability assessment for machines' component status is set to 'On'	□	□
3.1.3.3	Ensure that 'Endpoint protection' component status is set to 'On'	□	□
3.1.3.4	Ensure that 'Agentless scanning for machines' component status is set to 'On'	□	□
3.1.3.5	Ensure that 'File Integrity Monitoring' component status is set to 'On'	□	□
3.1.4.1	Ensure That Microsoft Defender for Containers Is Set To 'On'	□	□
3.1.4.2	Ensure that 'Agentless discovery for Kubernetes' component status 'On'	□	□
3.1.4.3	Ensure that 'Agentless container vulnerability assessment' component status is 'On'	□	□
3.1.5.1	Ensure That Microsoft Defender for Storage Is Set To 'On'	□	□
3.1.6.1	Ensure That Microsoft Defender for App Services Is Set To 'On'	□	□
3.1.7.1	Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On'	□	□
3.1.7.2	Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On'	□	□
3.1.7.3	Ensure That Microsoft Defender for (Managed Instance) Azure SQL Databases Is Set To 'On'	□	□
3.1.7.4	Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On'	□	□
3.1.8.1	Ensure That Microsoft Defender for Key Vault Is Set To 'On'	□	□

Recommendation		Set Correctly	
		Yes	No
3.1.9.1	Ensure That Microsoft Defender for Resource Manager Is Set To 'On'	□	□
3.1.10	Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed'	□	□
3.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'	□	□
3.1.12	Ensure That 'All users with the following roles' is set to 'Owner'	□	□
3.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email	□	□
3.1.14	Ensure That 'Notify about alerts with the following severity' is Set to 'High'	□	□
3.1.15	Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled	□	□
3.1.16	[LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On'	□	□
3.2.1	Ensure That Microsoft Defender for IoT Hub Is Set To 'On'	□	□
3.3.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults	□	□
3.3.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults.	□	□
3.3.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	□	□
3.3.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults	□	□
3.3.5	Ensure the Key Vault is Recoverable	□	□
3.3.6	Enable Role Based Access Control for Azure Key Vault	□	□
3.3.7	Ensure that Private Endpoints are Used for Azure Key Vault	□	□
3.3.8	Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services	□	□
4.1	Ensure that 'Secure transfer required' is set to 'Enabled'	□	□
4.2	Ensure that ‘Enable Infrastructure Encryption’ for Each Storage Account in Azure Storage is Set to ‘enabled’	□	□

Recommendation		Set Correctly	
		Yes	No
4.3	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	□	□
4.4	Ensure that Storage Account Access Keys are Periodically Regenerated	□	□
4.5	Ensure that Shared Access Signature Tokens Expire Within an Hour	□	□
4.6	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	□	□
4.7	Ensure Default Network Access Rule for Storage Accounts is Set to Deny	□	□
4.8	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	□	□
4.9	Ensure Private Endpoints are used to access Storage Accounts	□	□
4.10	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	□	□
4.11	Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK)	□	□
4.12	Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests	□	□
4.13	Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests	□	□
4.14	Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests	□	□
4.15	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	□	□
4.16	Ensure 'Cross Tenant Replication' is not enabled	□	□
4.17	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	□	□
5.1.1	Ensure that 'Auditing' is set to 'On'	□	□
5.1.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	□	□
5.1.3	Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key	□	□

Recommendation		Set Correctly	
		Yes	No
5.1.4	Ensure that Microsoft Entra authentication is Configured for SQL Servers	□	□
5.1.5	Ensure that 'Data encryption' is set to 'On' on a SQL Database	□	□
5.1.6	Ensure that 'Auditing' Retention is 'greater than 90 days'	□	□
5.1.7	Ensure Public Network Access is Disabled	□	□
5.2.1	Ensure server parameter 'require_secure_transport' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.2	Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.3	Ensure server parameter 'connection_throttle.enable' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.4	Ensure server parameter 'logfiles.retention_days' is greater than 3 days for PostgreSQL flexible server	□	□
5.2.5	Ensure 'Allow public access from any Azure service within Azure to this server' for PostgreSQL flexible server is disabled	□	□
5.2.6	[LEGACY] Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL single server	□	□
5.2.7	[LEGACY] Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL single server	□	□
5.2.8	[LEGACY] Ensure 'Infrastructure double encryption' for PostgreSQL single server is 'Enabled'	□	□
5.3.1	Ensure server parameter 'require_secure_transport' is set to 'ON' for MySQL flexible server	□	□
5.3.2	Ensure server parameter 'tls_version' is set to 'TLSv1.2' (or higher) for MySQL flexible server	□	□
5.3.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL flexible server	□	□
5.3.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL flexible server	□	□
5.4.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	□	□
5.4.2	Ensure That Private Endpoints Are Used Where Possible	□	□
5.4.3	Use Entra ID Client Authentication and Azure RBAC where possible	□	□

Recommendation		Set Correctly	
		Yes	No
6.1.1	Ensure that a 'Diagnostic Setting' exists for Subscription Activity Logs	□	□
6.1.2	Ensure Diagnostic Setting captures appropriate categories	□	□
6.1.3	Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (CMK)	□	□
6.1.4	Ensure that logging for Azure Key Vault is 'Enabled'	□	□
6.1.5	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics	□	□
6.1.6	Ensure that logging for Azure AppService 'HTTP logs' is enabled	□	□
6.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment	□	□
6.2.2	Ensure that Activity Log Alert exists for Delete Policy Assignment	□	□
6.2.3	Ensure that Activity Log Alert exists for Create or Update Network Security Group	□	□
6.2.4	Ensure that Activity Log Alert exists for Delete Network Security Group	□	□
6.2.5	Ensure that Activity Log Alert exists for Create or Update Security Solution	□	□
6.2.6	Ensure that Activity Log Alert exists for Delete Security Solution	□	□
6.2.7	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule	□	□
6.2.8	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule	□	□
6.2.9	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule	□	□
6.2.10	Ensure that Activity Log Alert exists for Delete Public IP Address rule	□	□
6.3.1	Ensure Application Insights are Configured	□	□
6.4	Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it	□	□

Recommendation		Set Correctly	
		Yes	No
6.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)	□	□
7.1	Ensure that RDP access from the Internet is evaluated and restricted	□	□
7.2	Ensure that SSH access from the Internet is evaluated and restricted	□	□
7.3	Ensure that UDP access from the Internet is evaluated and restricted	□	□
7.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted	□	□
7.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'	□	□
7.6	Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use	□	□
7.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis	□	□
8.1	Ensure an Azure Bastion Host Exists	□	□
8.2	Ensure Virtual Machines are utilizing Managed Disks	□	□
8.3	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)	□	□
8.4	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK)	□	□
8.5	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks'	□	□
8.6	Ensure that 'Enable Data Access Authentication Mode' is 'Checked'	□	□
8.7	Ensure that Only Approved Extensions Are Installed	□	□
8.8	Ensure that Endpoint Protection for all Virtual Machines is installed	□	□
8.9	[Legacy] Ensure that VHDs are Encrypted	□	□
8.10	Ensure only MFA enabled identities can access privileged Virtual Machine	□	□
8.11	Ensure Trusted Launch is enabled on Virtual Machines	□	□
9.1	Ensure 'HTTPS Only' is set to `On`	□	□

Recommendation		Set Correctly	
		Yes	No
9.2	Ensure App Service Authentication is set up for apps in Azure App Service	□	□
9.3	Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled'	□	□
9.4	Ensure Web App is using the latest version of TLS encryption	□	□
9.5	Ensure that Register with Entra ID is enabled on App Service	□	□
9.6	Ensure that 'Basic Authentication' is 'Disabled'	□	□
9.7	Ensure that 'PHP version' is currently supported (if in use)	□	□
9.8	Ensure that 'Python version' is currently supported (if in use)	□	□
9.9	Ensure that 'Java version' is currently supported (if in use)	□	□
9.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use)	□	□
9.11	Ensure Azure Key Vaults are Used to Store Secrets	□	□
9.12	Ensure that 'Remote debugging' is set to 'Off'	□	□
10.1	Ensure that Resource Locks are set for Mission-Critical Azure Resources	□	□

Appendix: CIS Controls v7 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.6	Ensure that account 'Lockout Threshold' is less than or equal to '10'	□	□
2.7	Ensure that account 'Lockout duration in seconds' is greater than or equal to '60'	□	□

Appendix: CIS Controls v8 IG 1 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure Security Defaults is enabled on Microsoft Entra ID	□	□
2.1.2	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users	□	□
2.1.3	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users	□	□
2.1.4	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled	□	□
2.2.3	Ensure that an exclusionary Device code flow policy is considered	□	□
2.2.4	Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups	□	□
2.2.5	Ensure that A Multi-factor Authentication Policy Exists for All Users	□	□
2.2.6	Ensure Multi-factor Authentication is Required for Risky Sign-ins	□	□
2.2.7	Ensure Multi-factor Authentication is Required for Windows Azure Service Management API	□	□
2.2.8	Ensure Multi-factor Authentication is Required to access Microsoft Admin Portals	□	□
2.4	Ensure Guest Users Are Reviewed on a Regular Basis	□	□
2.5	Ensure That 'Number of methods required to reset' is set to '2'	□	□
2.8	Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization	□	□
2.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	□	□
2.11	Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes'	□	□
2.12	Ensure `User consent for applications` is set to `Do not allow user consent`	□	□

Recommendation		Set Correctly	
		Yes	No
2.13	Ensure ‘User consent for applications’ Is Set To ‘Allow for Verified Publishers’	□	□
2.14	Ensure That ‘Users Can Register Applications’ Is Set to ‘No’	□	□
2.15	Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	□	□
2.16	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'	□	□
2.17	Ensure That 'Restrict access to Microsoft Entra admin center' is Set to 'Yes'	□	□
2.22	Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes'	□	□
2.23	Ensure That No Custom Subscription Administrator Roles Exist	□	□
2.24	Ensure a Custom Role is Assigned Permissions for Administering Resource Locks	□	□
2.25	Ensure That 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' Is Set To 'Permit no one'	□	□
2.26	Ensure fewer than 5 users have global administrator assignment	□	□
3.1.3.1	Ensure That Microsoft Defender for Servers Is Set to 'On'	□	□
3.1.3.3	Ensure that 'Endpoint protection' component status is set to 'On'	□	□
3.1.9.1	Ensure That Microsoft Defender for Resource Manager Is Set To 'On'	□	□
3.1.10	Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed'	□	□
3.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'	□	□
3.1.12	Ensure That 'All users with the following roles' is set to 'Owner'	□	□
3.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email	□	□

Recommendation		Set Correctly	
		Yes	No
3.3.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults	□	□
3.3.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults.	□	□
3.3.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	□	□
3.3.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults	□	□
3.3.5	Ensure the Key Vault is Recoverable	□	□
3.3.6	Enable Role Based Access Control for Azure Key Vault	□	□
3.3.8	Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services	□	□
4.3	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	□	□
4.4	Ensure that Storage Account Access Keys are Periodically Regenerated	□	□
4.5	Ensure that Shared Access Signature Tokens Expire Within an Hour	□	□
4.6	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	□	□
4.8	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	□	□
4.10	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	□	□
4.16	Ensure 'Cross Tenant Replication' is not enabled	□	□
4.17	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	□	□
5.1.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	□	□
5.1.6	Ensure that 'Auditing' Retention is 'greater than 90 days'	□	□
5.1.7	Ensure Public Network Access is Disabled	□	□
5.2.2	Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL flexible server	□	□

Recommendation		Set Correctly	
		Yes	No
5.2.3	Ensure server parameter 'connection_throttle.enable' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.4	Ensure server parameter 'logfiles.retention_days' is greater than 3 days for PostgreSQL flexible server	□	□
5.2.5	Ensure 'Allow public access from any Azure service within Azure to this server' for PostgreSQL flexible server is disabled	□	□
5.2.6	[LEGACY] Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL single server	□	□
5.2.7	[LEGACY] Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL single server	□	□
5.3.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL flexible server	□	□
5.3.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL flexible server	□	□
5.4.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	□	□
6.3.1	Ensure Application Insights are Configured	□	□
6.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)	□	□
7.1	Ensure that RDP access from the Internet is evaluated and restricted	□	□
7.2	Ensure that SSH access from the Internet is evaluated and restricted	□	□
7.3	Ensure that UDP access from the Internet is evaluated and restricted	□	□
7.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted	□	□
7.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'	□	□
7.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis	□	□
8.1	Ensure an Azure Bastion Host Exists	□	□
8.5	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks'	□	□

Recommendation		Set Correctly	
		Yes	No
8.6	Ensure that 'Enable Data Access Authentication Mode' is 'Checked'	□	□
8.7	Ensure that Only Approved Extensions Are Installed	□	□
8.8	Ensure that Endpoint Protection for all Virtual Machines is installed	□	□
8.10	Ensure only MFA enabled identities can access privileged Virtual Machine	□	□
8.11	Ensure Trusted Launch is enabled on Virtual Machines	□	□
9.2	Ensure App Service Authentication is set up for apps in Azure App Service	□	□
9.7	Ensure that 'PHP version' is currently supported (if in use)	□	□
9.8	Ensure that 'Python version' is currently supported (if in use)	□	□
9.9	Ensure that 'Java version' is currently supported (if in use)	□	□
9.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use)	□	□
9.11	Ensure Azure Key Vaults are Used to Store Secrets	□	□
10.1	Ensure that Resource Locks are set for Mission-Critical Azure Resources	□	□

Appendix: CIS Controls v8 IG 2 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure Security Defaults is enabled on Microsoft Entra ID	□	□
2.1.2	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users	□	□
2.1.3	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users	□	□
2.1.4	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled	□	□
2.2.1	Ensure Trusted Locations Are Defined	□	□
2.2.2	Ensure that an exclusionary Geographic Access Policy is considered	□	□
2.2.3	Ensure that an exclusionary Device code flow policy is considered	□	□
2.2.4	Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups	□	□
2.2.5	Ensure that A Multi-factor Authentication Policy Exists for All Users	□	□
2.2.6	Ensure Multi-factor Authentication is Required for Risky Sign-ins	□	□
2.2.7	Ensure Multi-factor Authentication is Required for Windows Azure Service Management API	□	□
2.2.8	Ensure Multi-factor Authentication is Required to access Microsoft Admin Portals	□	□
2.4	Ensure Guest Users Are Reviewed on a Regular Basis	□	□
2.5	Ensure That 'Number of methods required to reset' is set to '2'	□	□
2.6	Ensure that account 'Lockout Threshold' is less than or equal to '10'	□	□
2.7	Ensure that account 'Lockout duration in seconds' is greater than or equal to '60'	□	□

Recommendation		Set Correctly	
		Yes	No
2.8	Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization	□	□
2.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	□	□
2.10	Ensure that 'Notify users on password resets?' is set to 'Yes'	□	□
2.11	Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes'	□	□
2.12	Ensure `User consent for applications` is set to `Do not allow user consent`	□	□
2.13	Ensure ‘User consent for applications’ Is Set To ‘Allow for Verified Publishers’	□	□
2.14	Ensure That ‘Users Can Register Applications’ Is Set to ‘No’	□	□
2.15	Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	□	□
2.16	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'	□	□
2.17	Ensure That 'Restrict access to Microsoft Entra admin center' is Set to 'Yes'	□	□
2.22	Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes'	□	□
2.23	Ensure That No Custom Subscription Administrator Roles Exist	□	□
2.24	Ensure a Custom Role is Assigned Permissions for Administering Resource Locks	□	□
2.25	Ensure That 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' Is Set To 'Permit no one'	□	□
2.26	Ensure fewer than 5 users have global administrator assignment	□	□
3.1.1.1	Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On'	□	□
3.1.1.2	Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected	□	□

Recommendation		Set Correctly	
		Yes	No
3.1.3.1	Ensure That Microsoft Defender for Servers Is Set to 'On'	□	□
3.1.3.2	Ensure that 'Vulnerability assessment for machines' component status is set to 'On'	□	□
3.1.3.3	Ensure that 'Endpoint protection' component status is set to 'On'	□	□
3.1.3.4	Ensure that 'Agentless scanning for machines' component status is set to 'On'	□	□
3.1.3.5	Ensure that 'File Integrity Monitoring' component status is set to 'On'	□	□
3.1.4.1	Ensure That Microsoft Defender for Containers Is Set To 'On'	□	□
3.1.4.2	Ensure that 'Agentless discovery for Kubernetes' component status 'On'	□	□
3.1.4.3	Ensure that 'Agentless container vulnerability assessment' component status is 'On'	□	□
3.1.5.1	Ensure That Microsoft Defender for Storage Is Set To 'On'	□	□
3.1.6.1	Ensure That Microsoft Defender for App Services Is Set To 'On'	□	□
3.1.7.1	Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On'	□	□
3.1.7.2	Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On'	□	□
3.1.7.3	Ensure That Microsoft Defender for (Managed Instance) Azure SQL Databases Is Set To 'On'	□	□
3.1.7.4	Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On'	□	□
3.1.8.1	Ensure That Microsoft Defender for Key Vault Is Set To 'On'	□	□
3.1.9.1	Ensure That Microsoft Defender for Resource Manager Is Set To 'On'	□	□
3.1.10	Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed'	□	□
3.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'	□	□

Recommendation		Set Correctly	
		Yes	No
3.1.12	Ensure That 'All users with the following roles' is set to 'Owner'	□	□
3.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email	□	□
3.1.15	Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled	□	□
3.1.16	[LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On'	□	□
3.2.1	Ensure That Microsoft Defender for IoT Hub Is Set To 'On'	□	□
3.3.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults	□	□
3.3.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults.	□	□
3.3.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	□	□
3.3.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults	□	□
3.3.5	Ensure the Key Vault is Recoverable	□	□
3.3.6	Enable Role Based Access Control for Azure Key Vault	□	□
3.3.7	Ensure that Private Endpoints are Used for Azure Key Vault	□	□
3.3.8	Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services	□	□
4.1	Ensure that 'Secure transfer required' is set to 'Enabled'	□	□
4.2	Ensure that ‘Enable Infrastructure Encryption’ for Each Storage Account in Azure Storage is Set to ‘enabled’	□	□
4.3	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	□	□
4.4	Ensure that Storage Account Access Keys are Periodically Regenerated	□	□
4.5	Ensure that Shared Access Signature Tokens Expire Within an Hour	□	□
4.6	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	□	□

Recommendation		Set Correctly	
		Yes	No
4.7	Ensure Default Network Access Rule for Storage Accounts is Set to Deny	□	□
4.8	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	□	□
4.9	Ensure Private Endpoints are used to access Storage Accounts	□	□
4.10	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	□	□
4.11	Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK)	□	□
4.12	Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests	□	□
4.13	Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests	□	□
4.14	Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests	□	□
4.15	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	□	□
4.16	Ensure 'Cross Tenant Replication' is not enabled	□	□
4.17	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	□	□
5.1.1	Ensure that 'Auditing' is set to 'On'	□	□
5.1.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	□	□
5.1.3	Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key	□	□
5.1.4	Ensure that Microsoft Entra authentication is Configured for SQL Servers	□	□
5.1.5	Ensure that 'Data encryption' is set to 'On' on a SQL Database	□	□
5.1.6	Ensure that 'Auditing' Retention is 'greater than 90 days'	□	□
5.1.7	Ensure Public Network Access is Disabled	□	□
5.2.1	Ensure server parameter 'require_secure_transport' is set to 'ON' for PostgreSQL flexible server	□	□

Recommendation		Set Correctly	
		Yes	No
5.2.2	Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.3	Ensure server parameter 'connection_throttle.enable' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.4	Ensure server parameter 'logfiles.retention_days' is greater than 3 days for PostgreSQL flexible server	□	□
5.2.5	Ensure 'Allow public access from any Azure service within Azure to this server' for PostgreSQL flexible server is disabled	□	□
5.2.6	[LEGACY] Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL single server	□	□
5.2.7	[LEGACY] Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL single server	□	□
5.2.8	[LEGACY] Ensure 'Infrastructure double encryption' for PostgreSQL single server is 'Enabled'	□	□
5.3.1	Ensure server parameter 'require_secure_transport' is set to 'ON' for MySQL flexible server	□	□
5.3.2	Ensure server parameter 'tls_version' is set to 'TLSv1.2' (or higher) for MySQL flexible server	□	□
5.3.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL flexible server	□	□
5.3.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL flexible server	□	□
5.4.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	□	□
5.4.2	Ensure That Private Endpoints Are Used Where Possible	□	□
5.4.3	Use Entra ID Client Authentication and Azure RBAC where possible	□	□
6.1.1	Ensure that a 'Diagnostic Setting' exists for Subscription Activity Logs	□	□
6.1.2	Ensure Diagnostic Setting captures appropriate categories	□	□
6.1.3	Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (CMK)	□	□
6.1.4	Ensure that logging for Azure Key Vault is 'Enabled'	□	□

Recommendation		Set Correctly	
		Yes	No
6.1.5	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics	□	□
6.1.6	Ensure that logging for Azure AppService 'HTTP logs' is enabled	□	□
6.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment	□	□
6.2.2	Ensure that Activity Log Alert exists for Delete Policy Assignment	□	□
6.2.3	Ensure that Activity Log Alert exists for Create or Update Network Security Group	□	□
6.2.4	Ensure that Activity Log Alert exists for Delete Network Security Group	□	□
6.2.5	Ensure that Activity Log Alert exists for Create or Update Security Solution	□	□
6.2.6	Ensure that Activity Log Alert exists for Delete Security Solution	□	□
6.2.7	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule	□	□
6.2.8	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule	□	□
6.2.9	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule	□	□
6.2.10	Ensure that Activity Log Alert exists for Delete Public IP Address rule	□	□
6.3.1	Ensure Application Insights are Configured	□	□
6.4	Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it	□	□
6.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)	□	□
7.1	Ensure that RDP access from the Internet is evaluated and restricted	□	□
7.2	Ensure that SSH access from the Internet is evaluated and restricted	□	□
7.3	Ensure that UDP access from the Internet is evaluated and restricted	□	□

Recommendation		Set Correctly	
		Yes	No
7.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted	□	□
7.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'	□	□
7.6	Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use	□	□
7.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis	□	□
8.1	Ensure an Azure Bastion Host Exists	□	□
8.2	Ensure Virtual Machines are utilizing Managed Disks	□	□
8.3	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)	□	□
8.4	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK)	□	□
8.5	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks'	□	□
8.6	Ensure that 'Enable Data Access Authentication Mode' is 'Checked'	□	□
8.7	Ensure that Only Approved Extensions Are Installed	□	□
8.8	Ensure that Endpoint Protection for all Virtual Machines is installed	□	□
8.9	[Legacy] Ensure that VHDs are Encrypted	□	□
8.10	Ensure only MFA enabled identities can access privileged Virtual Machine	□	□
8.11	Ensure Trusted Launch is enabled on Virtual Machines	□	□
9.1	Ensure 'HTTPS Only' is set to `On`	□	□
9.2	Ensure App Service Authentication is set up for apps in Azure App Service	□	□
9.3	Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled'	□	□
9.4	Ensure Web App is using the latest version of TLS encryption	□	□
9.5	Ensure that Register with Entra ID is enabled on App Service	□	□
9.6	Ensure that 'Basic Authentication' is 'Disabled'	□	□

Recommendation		Set Correctly	
		Yes	No
9.7	Ensure that 'PHP version' is currently supported (if in use)	□	□
9.8	Ensure that 'Python version' is currently supported (if in use)	□	□
9.9	Ensure that 'Java version' is currently supported (if in use)	□	□
9.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use)	□	□
9.11	Ensure Azure Key Vaults are Used to Store Secrets	□	□
9.12	Ensure that 'Remote debugging' is set to 'Off'	□	□
10.1	Ensure that Resource Locks are set for Mission-Critical Azure Resources	□	□

Appendix: CIS Controls v8 IG 3 Mapped Recommendations

Recommendation		Set Correctly	
		Yes	No
2.1.1	Ensure Security Defaults is enabled on Microsoft Entra ID	□	□
2.1.2	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users	□	□
2.1.3	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users	□	□
2.1.4	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled	□	□
2.2.1	Ensure Trusted Locations Are Defined	□	□
2.2.2	Ensure that an exclusionary Geographic Access Policy is considered	□	□
2.2.3	Ensure that an exclusionary Device code flow policy is considered	□	□
2.2.4	Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups	□	□
2.2.5	Ensure that A Multi-factor Authentication Policy Exists for All Users	□	□
2.2.6	Ensure Multi-factor Authentication is Required for Risky Sign-ins	□	□
2.2.7	Ensure Multi-factor Authentication is Required for Windows Azure Service Management API	□	□
2.2.8	Ensure Multi-factor Authentication is Required to access Microsoft Admin Portals	□	□
2.3	Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes'	□	□
2.4	Ensure Guest Users Are Reviewed on a Regular Basis	□	□
2.5	Ensure That 'Number of methods required to reset' is set to '2'	□	□
2.6	Ensure that account 'Lockout Threshold' is less than or equal to '10'	□	□

Recommendation		Set Correctly	
		Yes	No
2.7	Ensure that account 'Lockout duration in seconds' is greater than or equal to '60'	□	□
2.8	Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization	□	□
2.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0'	□	□
2.10	Ensure that 'Notify users on password resets?' is set to 'Yes'	□	□
2.11	Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes'	□	□
2.12	Ensure `User consent for applications` is set to `Do not allow user consent`	□	□
2.13	Ensure ‘User consent for applications’ Is Set To ‘Allow for Verified Publishers’	□	□
2.14	Ensure That ‘Users Can Register Applications’ Is Set to ‘No’	□	□
2.15	Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects'	□	□
2.16	Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users'	□	□
2.17	Ensure That 'Restrict access to Microsoft Entra admin center' is Set to 'Yes'	□	□
2.18	Ensure that 'Restrict user ability to access groups features in the Access Pane' is Set to 'Yes'	□	□
2.19	Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No'	□	□
2.20	Ensure that 'Owners can manage group membership requests in My Groups' is set to 'No'	□	□
2.21	Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No'	□	□
2.22	Ensure that 'Require Multifactor Authentication to register or join devices with Microsoft Entra' is set to 'Yes'	□	□
2.23	Ensure That No Custom Subscription Administrator Roles Exist	□	□

Recommendation		Set Correctly	
		Yes	No
2.24	Ensure a Custom Role is Assigned Permissions for Administering Resource Locks	□	□
2.25	Ensure That 'Subscription leaving Microsoft Entra tenant' and 'Subscription entering Microsoft Entra tenant' Is Set To 'Permit no one'	□	□
2.26	Ensure fewer than 5 users have global administrator assignment	□	□
3.1.1.1	Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On'	□	□
3.1.1.2	Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected	□	□
3.1.3.1	Ensure That Microsoft Defender for Servers Is Set to 'On'	□	□
3.1.3.2	Ensure that 'Vulnerability assessment for machines' component status is set to 'On'	□	□
3.1.3.3	Ensure that 'Endpoint protection' component status is set to 'On'	□	□
3.1.3.4	Ensure that 'Agentless scanning for machines' component status is set to 'On'	□	□
3.1.3.5	Ensure that 'File Integrity Monitoring' component status is set to 'On'	□	□
3.1.4.1	Ensure That Microsoft Defender for Containers Is Set To 'On'	□	□
3.1.4.2	Ensure that 'Agentless discovery for Kubernetes' component status 'On'	□	□
3.1.4.3	Ensure that 'Agentless container vulnerability assessment' component status is 'On'	□	□
3.1.5.1	Ensure That Microsoft Defender for Storage Is Set To 'On'	□	□
3.1.6.1	Ensure That Microsoft Defender for App Services Is Set To 'On'	□	□
3.1.7.1	Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On'	□	□
3.1.7.2	Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On'	□	□
3.1.7.3	Ensure That Microsoft Defender for (Managed Instance) Azure SQL Databases Is Set To 'On'	□	□

Recommendation		Set Correctly	
		Yes	No
3.1.7.4	Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On'	□	□
3.1.8.1	Ensure That Microsoft Defender for Key Vault Is Set To 'On'	□	□
3.1.9.1	Ensure That Microsoft Defender for Resource Manager Is Set To 'On'	□	□
3.1.10	Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed'	□	□
3.1.11	Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled'	□	□
3.1.12	Ensure That 'All users with the following roles' is set to 'Owner'	□	□
3.1.13	Ensure 'Additional email addresses' is Configured with a Security Contact Email	□	□
3.1.14	Ensure That 'Notify about alerts with the following severity' is Set to 'High'	□	□
3.1.15	Ensure that Microsoft Defender External Attack Surface Monitoring (EASM) is enabled	□	□
3.1.16	[LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On'	□	□
3.2.1	Ensure That Microsoft Defender for IoT Hub Is Set To 'On'	□	□
3.3.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults	□	□
3.3.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults.	□	□
3.3.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults	□	□
3.3.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults	□	□
3.3.5	Ensure the Key Vault is Recoverable	□	□
3.3.6	Enable Role Based Access Control for Azure Key Vault	□	□
3.3.7	Ensure that Private Endpoints are Used for Azure Key Vault	□	□
3.3.8	Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services	□	□

Recommendation		Set Correctly	
		Yes	No
4.1	Ensure that 'Secure transfer required' is set to 'Enabled'	□	□
4.2	Ensure that ‘Enable Infrastructure Encryption’ for Each Storage Account in Azure Storage is Set to ‘enabled’	□	□
4.3	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account	□	□
4.4	Ensure that Storage Account Access Keys are Periodically Regenerated	□	□
4.5	Ensure that Shared Access Signature Tokens Expire Within an Hour	□	□
4.6	Ensure that 'Public Network Access' is 'Disabled' for storage accounts	□	□
4.7	Ensure Default Network Access Rule for Storage Accounts is Set to Deny	□	□
4.8	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access	□	□
4.9	Ensure Private Endpoints are used to access Storage Accounts	□	□
4.10	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage	□	□
4.11	Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK)	□	□
4.12	Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests	□	□
4.13	Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests	□	□
4.14	Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests	□	□
4.15	Ensure the 'Minimum TLS version' for storage accounts is set to 'Version 1.2'	□	□
4.16	Ensure 'Cross Tenant Replication' is not enabled	□	□
4.17	Ensure that 'Allow Blob Anonymous Access' is set to 'Disabled'	□	□
5.1.1	Ensure that 'Auditing' is set to 'On'	□	□
5.1.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP)	□	□

Recommendation		Set Correctly	
		Yes	No
5.1.3	Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key	□	□
5.1.4	Ensure that Microsoft Entra authentication is Configured for SQL Servers	□	□
5.1.5	Ensure that 'Data encryption' is set to 'On' on a SQL Database	□	□
5.1.6	Ensure that 'Auditing' Retention is 'greater than 90 days'	□	□
5.1.7	Ensure Public Network Access is Disabled	□	□
5.2.1	Ensure server parameter 'require_secure_transport' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.2	Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.3	Ensure server parameter 'connection_throttle.enable' is set to 'ON' for PostgreSQL flexible server	□	□
5.2.4	Ensure server parameter 'logfiles.retention_days' is greater than 3 days for PostgreSQL flexible server	□	□
5.2.5	Ensure 'Allow public access from any Azure service within Azure to this server' for PostgreSQL flexible server is disabled	□	□
5.2.6	[LEGACY] Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL single server	□	□
5.2.7	[LEGACY] Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL single server	□	□
5.2.8	[LEGACY] Ensure 'Infrastructure double encryption' for PostgreSQL single server is 'Enabled'	□	□
5.3.1	Ensure server parameter 'require_secure_transport' is set to 'ON' for MySQL flexible server	□	□
5.3.2	Ensure server parameter 'tls_version' is set to 'TLSv1.2' (or higher) for MySQL flexible server	□	□
5.3.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL flexible server	□	□
5.3.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL flexible server	□	□
5.4.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks	□	□
5.4.2	Ensure That Private Endpoints Are Used Where Possible	□	□

Recommendation		Set Correctly	
		Yes	No
5.4.3	Use Entra ID Client Authentication and Azure RBAC where possible	□	□
6.1.1	Ensure that a 'Diagnostic Setting' exists for Subscription Activity Logs	□	□
6.1.2	Ensure Diagnostic Setting captures appropriate categories	□	□
6.1.3	Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (CMK)	□	□
6.1.4	Ensure that logging for Azure Key Vault is 'Enabled'	□	□
6.1.5	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics	□	□
6.1.6	Ensure that logging for Azure AppService 'HTTP logs' is enabled	□	□
6.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment	□	□
6.2.2	Ensure that Activity Log Alert exists for Delete Policy Assignment	□	□
6.2.3	Ensure that Activity Log Alert exists for Create or Update Network Security Group	□	□
6.2.4	Ensure that Activity Log Alert exists for Delete Network Security Group	□	□
6.2.5	Ensure that Activity Log Alert exists for Create or Update Security Solution	□	□
6.2.6	Ensure that Activity Log Alert exists for Delete Security Solution	□	□
6.2.7	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule	□	□
6.2.8	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule	□	□
6.2.9	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule	□	□
6.2.10	Ensure that Activity Log Alert exists for Delete Public IP Address rule	□	□
6.3.1	Ensure Application Insights are Configured	□	□

Recommendation		Set Correctly	
		Yes	No
6.4	Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it	□	□
6.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads)	□	□
7.1	Ensure that RDP access from the Internet is evaluated and restricted	□	□
7.2	Ensure that SSH access from the Internet is evaluated and restricted	□	□
7.3	Ensure that UDP access from the Internet is evaluated and restricted	□	□
7.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted	□	□
7.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'	□	□
7.6	Ensure that Network Watcher is 'Enabled' for Azure Regions that are in use	□	□
7.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis	□	□
8.1	Ensure an Azure Bastion Host Exists	□	□
8.2	Ensure Virtual Machines are utilizing Managed Disks	□	□
8.3	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK)	□	□
8.4	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK)	□	□
8.5	Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks'	□	□
8.6	Ensure that 'Enable Data Access Authentication Mode' is 'Checked'	□	□
8.7	Ensure that Only Approved Extensions Are Installed	□	□
8.8	Ensure that Endpoint Protection for all Virtual Machines is installed	□	□
8.9	[Legacy] Ensure that VHDs are Encrypted	□	□
8.10	Ensure only MFA enabled identities can access privileged Virtual Machine	□	□

Recommendation		Set Correctly	
		Yes	No
8.11	Ensure Trusted Launch is enabled on Virtual Machines	□	□
9.1	Ensure 'HTTPS Only' is set to `On`	□	□
9.2	Ensure App Service Authentication is set up for apps in Azure App Service	□	□
9.3	Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled'	□	□
9.4	Ensure Web App is using the latest version of TLS encryption	□	□
9.5	Ensure that Register with Entra ID is enabled on App Service	□	□
9.6	Ensure that 'Basic Authentication' is 'Disabled'	□	□
9.7	Ensure that 'PHP version' is currently supported (if in use)	□	□
9.8	Ensure that 'Python version' is currently supported (if in use)	□	□
9.9	Ensure that 'Java version' is currently supported (if in use)	□	□
9.10	Ensure that 'HTTP20enabled' is set to 'true' (if in use)	□	□
9.11	Ensure Azure Key Vaults are Used to Store Secrets	□	□
9.12	Ensure that 'Remote debugging' is set to 'Off'	□	□
10.1	Ensure that Resource Locks are set for Mission-Critical Azure Resources	□	□

Appendix: CIS Controls v8 Unmapped Recommendations

Recommendation		Set Correctly	
		Yes	No
	No unmapped recommendations to CIS Controls v8	□	□

Appendix: Change History

Date	Version	Changes for this version
Aug 28, 2024	3.0.0	ADD - Defender Cloud Security Posture Management - Text Subsection Article, No Recommendations (Ticket 18605)
Aug 28, 2024	3.0.0	ADD - Defender for API - Subsection Information Article, No Recommendations (Ticket 19125)
Aug 26, 2024	3.0.0	ADD - Ensure that account 'Lockout duration in seconds' is greater than or equal to '60' (Ticket 22443)
Aug 26, 2024	3.0.0	ADD - Ensure that account 'Lockout Threshold' is less than or equal to '10' (Ticket 22079)
Sep 5, 2024	3.0.0	ADD - Ensure that 'Agentless container vulnerability assessment' component status is 'On' (Ticket 22514)
Aug 30, 2024	3.0.0	ADD - Ensure that 'Agentless scanning for machines' component status is set to 'On' (Ticket 22474)
Aug 28, 2024	3.0.0	ADD - Ensure that an exclusionary Device code flow policy is considered (Ticket 21071)
Aug 19, 2024	3.0.0	ADD - Ensure that 'Basic Authentication' is 'Disabled' (Ticket 22383)
Aug 26, 2024	3.0.0	ADD - Ensure that 'Data Access Authentication Mode' is 'Disabled' (Ticket 20794)
Aug 21, 2024	3.0.0	ADD - Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks' (Ticket 22400)
Aug 30, 2024	3.0.0	ADD - Ensure that 'File Integrity Monitoring' component status is set to 'On' (Ticket 22475)
Aug 26, 2024	3.0.0	ADD - Ensure that 'Remote debugging' is set to 'Off' Draft (Ticket 22419)
Aug 16, 2024	3.0.0	ADD - Microsoft Cloud Security Posture Management - New Section (Ticket 22207)

Date	Version	Changes for this version
Aug 16, 2024	3.0.0	ADD - Microsoft Defender for APIs - New Section (Ticket 22222)
Feb 13, 2024	3.0.0	ADDED - Ensure Ensure that `Allow Blob Anonymous Access` is set to `Disabled` (Ticket 20640)
Aug 16, 2024	3.0.0	DELETE - Ensure that 'Users can add gallery apps to My Apps' is set to 'No' (Ticket 22199)
Jan 22, 2024	3.0.0	UPDATE - [LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On' - Updated to legacy with description indicating plan change (Ticket 20485)
Sep 3, 2024	3.0.0	UPDATE - 1.1.1 Ensure Security Defaults is enabled on Microsoft Entra ID Impact Description Update - Clarify that Conditional Access should be used instead if possible (Ticket 22140)
Sep 3, 2024	3.0.0	UPDATE - Add CLI Audit and Remediation commands and update Assessment Status to Automated - CLI and PowerShell commands added, status changed from manual to automated (Ticket 22423)
Sep 3, 2024	3.0.0	UPDATE - Add CLI Audit and Remediation commands and update Assessment Status to Automated - CLI and PowerShell commands added, status changed from manual to automated (Ticket 22424)
Aug 28, 2024	3.0.0	UPDATE - All - MSOL and Azure AD cmdlet references updated to use Graph PowerShell (Ticket 17315)
Sep 2, 2024	3.0.0	UPDATE - Audit Policy is a Community Policy, Not GA - Removed potentially destructive community Audit Policy (Ticket 22321)
Sep 2, 2024	3.0.0	UPDATE - Azure Portal and Azure CLI audit procedures are inconsistent - Updated Description, Rationale, Audit, and Remediation to clarify intent (Ticket 22242)
Sep 3, 2024	3.0.0	UPDATE - Classic roles may be deprecated by 09-2024 - Remove reference to classic roles, only mention custom roles (Ticket 19474)
Sep 3, 2024	3.0.0	UPDATE - CLI command missing closing quotation marks - CLI command updated (Ticket 22286)

Date	Version	Changes for this version
Aug 29, 2024	3.0.0	UPDATE - Conditional Access - All CA Recommendation profiles changed to "Level 2" (Ticket 22468)
Aug 28, 2024	3.0.0	UPDATE - Enable Role Based Access Control for Azure Key Vault - Assessment Status changed from Manual to Automated (Ticket 22438)
Aug 19, 2024	3.0.0	UPDATE - Enable Role Based Access Control for Azure Key Vault - Description, policy name, and parameter styling updated (Ticket 21900)
Aug 9, 2024	3.0.0	UPDATE - Ensure \`User consent for applications\` is set to \`Do not allow user consent\` - Updated MSOL commands to mggraph (Ticket 21705)
Aug 9, 2024	3.0.0	UPDATE - Ensure ‘User consent for applications’ Is Set To ‘Allow for Verified Publishers’ - Update msol powershell command to mggraph (Ticket 21704)
Aug 18, 2024	3.0.0	UPDATE - Ensure App Service Authentication is set up for apps in Azure App Service - Changes in CLI audit steps (Ticket 21096)
Aug 19, 2024	3.0.0	UPDATE - Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled' Draft - Title and Prose updated from "Ensure FTP deployments are Disabled" (Ticket 22378)
Aug 19, 2024	3.0.0	UPDATE - Ensure 'HTTPS Only' is set to 'On' - Retitled and updated from "Ensure Web App Redirects All HTTP traffic to HTTPS in Azure App Service" (Ticket 22376)
Sep 2, 2024	3.0.0	UPDATE - Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' - Marked as 'legacy', single server only (Ticket 22485)
Aug 9, 2024	3.0.0	UPDATE - Ensure Multi-factor Authentication is Required for Risky Sign-ins - Prose updated to reflect P2 licensing requirement (Ticket 22210)
Aug 27, 2024	3.0.0	UPDATE - Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) - Additional rationale context added (Ticket 22449)

Date	Version	Changes for this version
Aug 19, 2024	3.0.0	UPDATE - Ensure only MFA enabled identities can access privileged Virtual Machine - Automation status changed to Manual (Ticket 21897)
Sep 2, 2024	3.0.0	UPDATE - Ensure Private Endpoints are used to access Storage Accounts - Consider making level 2 to consider requirement for DNS entries - Updated Impact to reflect cost, changed from Level 1 to Level 2 (Ticket 22279)
Aug 28, 2024	3.0.0	UPDATE - Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server - References updated for Flexible Server (Ticket 21891)
Aug 28, 2024	3.0.0	UPDATE - Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server - References updated for Flexible Server (Ticket 21892)
Sep 2, 2024	3.0.0	UPDATE - Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL flexible server - Marked as 'legacy', single server only (Ticket 22483)
Sep 2, 2024	3.0.0	UPDATE - Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server - Marked as 'legacy', single server only (Ticket 22484)
Sep 2, 2024	3.0.0	UPDATE - Ensure Soft Delete is Enabled for Azure Containers and Blob Storage - Update Audit/Remediate from CLI and Default Value for accuracy (Ticket 22280)
Sep 2, 2024	3.0.0	UPDATE - Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK) - Update to Rationale explaining Manual Assessment Status (Ticket 22281)
Aug 29, 2024	3.0.0	UPDATE - Ensure that `Allow Blob Anonymous Access` is set to `Disabled` - Consider preview policy to replace the MODIFY policy being currently used. (Ticket 22282)
Aug 9, 2024	3.0.0	UPDATE - Ensure That ‘Users Can Register Applications’ Is Set to ‘No’ - Assessment status changed to Automated (Ticket 21747)

Date	Version	Changes for this version
Aug 9, 2024	3.0.0	UPDATE - Ensure That ‘Users Can Register Applications’ Is Set to ‘No’ - Update msol powershell command to mggraph (Ticket 21746)
Sep 2, 2024	3.0.0	UPDATE - Ensure that an exclusionary Geographic Access Policy is considered - Updated Azure AD cmdlets to Graph PowerShell (Ticket 22459)
Aug 26, 2024	3.0.0	UPDATE - Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks' - Added CLI & Powershell (Ticket 22413)
Aug 30, 2024	3.0.0	UPDATE - Ensure that 'Endpoint protection' component status is set to 'On' - Title changed, assessment status changed to Automated, prose updated for portal UI changes (Ticket 22417)
Jan 22, 2024	3.0.0	UPDATE - Ensure that Endpoint Protection for all Virtual Machines is installed - Newer policy ID added (Ticket 20579)
Aug 9, 2024	3.0.0	UPDATE - Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users' - Assessment status changed to Automated (Ticket 22307)
Aug 9, 2024	3.0.0	UPDATE - Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users' - Powershell audit and remediation procedures added (Ticket 21748)
Aug 9, 2024	3.0.0	UPDATE - Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' - Assessment changed to Automated (Ticket 21749)
Aug 9, 2024	3.0.0	UPDATE - Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' - Powershell updated to use mggraph (Ticket 21750)
Aug 23, 2024	3.0.0	UPDATE - Ensure that 'HTTP20enabled' is set to 'true' (if in use) - Prose updated to reflect 'app' or 'app services', not just 'web app' (Ticket 22273)

Date	Version	Changes for this version
Aug 19, 2024	3.0.0	UPDATE - Ensure that 'HTTP20enabled' is set to 'true' (if in use) - Title and Prose updated to reflect the setting name more accurately (Ticket 22379)
Aug 19, 2024	3.0.0	UPDATE - Ensure that 'Java version' is currently supported (if in use) - Changed from 'newest' to 'currently supported' release, updated title and prose (Ticket 22182)
Aug 23, 2024	3.0.0	UPDATE - Ensure that 'Java version' is currently supported (if in use) - Prose updated to reflect 'app' or 'app services', not just 'web app' (Ticket 22272)
Aug 3, 2024	3.0.0	UPDATE - Ensure That Microsoft Defender for Containers Is Set To 'On' - Description updated to highlight Defender for Containers features (Ticket 20486)
Jan 30, 2024	3.0.0	UPDATE - Ensure That Microsoft Defender for Key Vault Is Set To 'On' - Fixed CLI typo (Ticket 19004)
Jan 30, 2024	3.0.0	UPDATE - Ensure That Microsoft Defender for Resource Manager Is Set To 'On' - Fixed CLI typo (Ticket 19006)
Aug 9, 2024	3.0.0	UPDATE - Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users - Correct erroneous change to portal audit steps (Ticket 21073)
Sep 3, 2024	3.0.0	UPDATE - Ensure that Network Security Group Flow logs are captured and sent to Log Analytics - Clarity needed on Description and Audit Procedure - Recommendation updated for clarity (Ticket 17003)
Aug 19, 2024	3.0.0	UPDATE - Ensure that 'PHP version' is currently supported (if in use) - Changed from 'newest' to 'currently supported' release, updated title and prose (Ticket 22382)
Aug 19, 2024	3.0.0	UPDATE - Ensure that 'Python version' is currently supported (if in use) - Changed from 'newest' to 'currently supported' release, updated title and prose (Ticket 22381)

Date	Version	Changes for this version
Aug 16, 2024	3.0.0	UPDATE - Ensure that 'Require Multi-Factor Authentication to register or join devices with Microsoft Entra ID' is set to 'Yes' - Added links to CA Policy and updated description and rationale (Ticket 22308)
Aug 9, 2024	3.0.0	UPDATE - Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes' - Assessment status changed to Automated (Ticket 21745)
Aug 15, 2024	3.0.0	UPDATE - Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) - Syntax correction & addition (Ticket 22060)
Aug 19, 2024	3.0.0	UPDATE - Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults - Permission name corrected to 'List Secret' (Ticket 21899)
Aug 19, 2024	3.0.0	UPDATE - Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults - Permission name corrected to 'List Secret' (Ticket 21898)
Aug 19, 2024	3.0.0	UPDATE - Ensure the Key Vault is Recoverable - Added Azure Policy (Ticket 21395)
Sep 3, 2024	3.0.0	UPDATE - Ensure Trusted Locations Are Defined - Updated Azure AD cmdlets to Graph PowerShell (Ticket 22458)
Aug 28, 2024	3.0.0	UPDATE - Ensure Trusted Locations Are Defined - Updated prose to alert of MFA requirement for Break-Glass Accounts (Ticket 22385)
Aug 29, 2024	3.0.0	UPDATE - Key Vault - Section moved into "Security" parent category section (Ticket 22470)
Aug 30, 2024	3.0.0	UPDATE - Multiple Methods of Audit and Remediation - Information article updated to address Microsoft Graph PowerShell (Ticket 22467)
Sep 2, 2024	3.0.0	UPDATE - Need to review variations between "Single Server" and "Flexible Server" - PostgreSQL recommendations updated to align with flexible server (Ticket 17688)

Date	Version	Changes for this version
Sep 3, 2024	3.0.0	UPDATE - Please update Impact to consider new Microsoft best practice - Clarify that Conditional Access should be used instead if possible (Ticket 22141)
Sep 2, 2024	3.0.0	UPDATE - Propose updating the Assessment Status from Manual to Automated - Assessment Status changed from Manual to Automated (Ticket 22439)
Sep 2, 2024	3.0.0	UPDATE - Propose updating the Assessment Status from Manual to Automated - Assessment Status changed from Manual to Automated (Ticket 22442)
Sep 2, 2024	3.0.0	UPDATE - Proposing to update Assessment Status from Manual to Automated for "Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected" - Assessment Status changed from Manual to Automated (Ticket 22416)
Sep 2, 2024	3.0.0	UPDATE - Update Audit from Azure CLI steps, as 'application-insights' CLI extension is GA - Updated Audit CLI steps, command now GA (Ticket 22431)
Sep 2, 2024	3.0.0	UPDATE - Update Audit Procedure to include expected results - Updated audit from CLI command, added expected results for audit (Ticket 22440)
Sep 2, 2024	3.0.0	UPDATE - Update Audit Procedure to include expected results - Updated audit from CLI command, added expected results for audit (Ticket 22441)
Aug 28, 2024	3.0.0	UPDATE - Use Entra ID Client Authentication and Azure RBAC where possible - Policy added (Ticket 22320)

Date	Version	Changes for this version
Aug 28, 2024	3.0.0	ADD - Defender Cloud Security Posture Management - Text Subsection Article, No Recommendations (Ticket 18605)
Aug 28, 2024	3.0.0	ADD - Defender for API - Subsection Information Article, No Recommendations (Ticket 19125)
Aug 26, 2024	3.0.0	ADD - Ensure that account 'Lockout duration in seconds' is greater than or equal to '60' (Ticket 22443)
Aug 26, 2024	3.0.0	ADD - Ensure that account 'Lockout Threshold' is less than or equal to '10' (Ticket 22079)
Sep 5, 2024	3.0.0	ADD - Ensure that 'Agentless container vulnerability assessment' component status is 'On' (Ticket 22514)
Aug 30, 2024	3.0.0	ADD - Ensure that 'Agentless scanning for machines' component status is set to 'On' (Ticket 22474)
Aug 28, 2024	3.0.0	ADD - Ensure that an exclusionary Device code flow policy is considered (Ticket 21071)
Aug 19, 2024	3.0.0	ADD - Ensure that 'Basic Authentication' is 'Disabled' (Ticket 22383)
Aug 26, 2024	3.0.0	ADD - Ensure that 'Data Access Authentication Mode' is 'Disabled' (Ticket 20794)
Aug 21, 2024	3.0.0	ADD - Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks' (Ticket 22400)
Aug 30, 2024	3.0.0	ADD - Ensure that 'File Integrity Monitoring' component status is set to 'On' (Ticket 22475)
Aug 26, 2024	3.0.0	ADD - Ensure that 'Remote debugging' is set to 'Off' Draft (Ticket 22419)
Aug 16, 2024	3.0.0	ADD - Microsoft Cloud Security Posture Management - New Section (Ticket 22207)

Aug 16, 2024	3.0.0	ADD - Microsoft Defender for APIs - New Section (Ticket 22222)
Feb 13, 2024	3.0.0	ADDED - Ensure Ensure that `Allow Blob Anonymous Access` is set to `Disabled` (Ticket 20640)
Aug 16, 2024	3.0.0	DELETE - Ensure that 'Users can add gallery apps to My Apps' is set to 'No' (Ticket 22199)
Jan 22, 2024	3.0.0	UPDATE - [LEGACY] Ensure That Microsoft Defender for DNS Is Set To 'On' - Updated to legacy with description indicating plan change (Ticket 20485)
Sep 3, 2024	3.0.0	UPDATE - 1.1.1 Ensure Security Defaults is enabled on Microsoft Entra ID Impact Description Update - Clarify that Conditional Access should be used instead if possible (Ticket 22140)
Sep 3, 2024	3.0.0	UPDATE - Add CLI Audit and Remediation commands and update Assessment Status to Automated - CLI and PowerShell commands added, status changed from manual to automated (Ticket 22423)
Sep 3, 2024	3.0.0	UPDATE - Add CLI Audit and Remediation commands and update Assessment Status to Automated - CLI and PowerShell commands added, status changed from manual to automated (Ticket 22424)
Aug 28, 2024	3.0.0	UPDATE - All - MSOL and Azure AD cmdlet references updated to use Graph PowerShell (Ticket 17315)
Sep 2, 2024	3.0.0	UPDATE - Audit Policy is a Community Policy, Not GA - Removed potentially destructive community Audit Policy (Ticket 22321)
Sep 2, 2024	3.0.0	UPDATE - Azure Portal and Azure CLI audit procedures are inconsistent - Updated Description, Rationale, Audit, and Remediation to clarify intent (Ticket 22242)

Sep 3, 2024	3.0.0	UPDATE - Classic roles may be deprecated by 09-2024 - Remove reference to classic roles, only mention custom roles (Ticket 19474)
Sep 3, 2024	3.0.0	UPDATE - CLI command missing closing quotation marks - CLI command updated (Ticket 22286)
Aug 29, 2024	3.0.0	UPDATE - Conditional Access - All CA Recommendation profiles changed to "Level 2" (Ticket 22468)
Aug 28, 2024	3.0.0	UPDATE - Enable Role Based Access Control for Azure Key Vault - Assessment Status changed from Manual to Automated (Ticket 22438)
Aug 19, 2024	3.0.0	UPDATE - Enable Role Based Access Control for Azure Key Vault - Description, policy name, and parameter styling updated (Ticket 21900)
Aug 9, 2024	3.0.0	UPDATE - Ensure `User consent for applications` is set to `Do not allow user consent` - Updated MSOL commands to mggraph (Ticket 21705)
Aug 9, 2024	3.0.0	UPDATE - Ensure ‘User consent for applications’ Is Set To ‘Allow for Verified Publishers’ - Update msol powershell command to mggraph (Ticket 21704)
Aug 18, 2024	3.0.0	UPDATE - Ensure App Service Authentication is set up for apps in Azure App Service - Changes in CLI audit steps (Ticket 21096)
Aug 19, 2024	3.0.0	UPDATE - Ensure 'FTP State' is set to 'FTPS Only' or 'Disabled' Draft - Title and Prose updated from "Ensure FTP deployments are Disabled" (Ticket 22378)
Aug 19, 2024	3.0.0	UPDATE - Ensure 'HTTPS Only' is set to 'On' - Retitled and updated from "Ensure Web App Redirects All HTTP traffic to HTTPS in Azure App Service" (Ticket 22376)

Sep 2, 2024	3.0.0	UPDATE - Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' - Marked as 'legacy', single server only (Ticket 22485)
Aug 9, 2024	3.0.0	UPDATE - Ensure Multi-factor Authentication is Required for Risky Sign-ins - Prose updated to reflect P2 licensing requirement (Ticket 22210)
Aug 27, 2024	3.0.0	UPDATE - Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) - Additional rationale context added (Ticket 22449)
Aug 19, 2024	3.0.0	UPDATE - Ensure only MFA enabled identities can access privileged Virtual Machine - Automation status changed to Manual (Ticket 21897)
Sep 2, 2024	3.0.0	UPDATE - Ensure Private Endpoints are used to access Storage Accounts - Consider making level 2 to consider requirement for DNS entries - Updated Impact to reflect cost, changed from Level 1 to Level 2 (Ticket 22279)
Aug 28, 2024	3.0.0	UPDATE - Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server - References updated for Flexible Server (Ticket 21891)
Aug 28, 2024	3.0.0	UPDATE - Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server - References updated for Flexible Server (Ticket 21892)
Sep 2, 2024	3.0.0	UPDATE - Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL flexible server - Marked as 'legacy', single server only (Ticket 22483)

Sep 2, 2024	3.0.0	UPDATE - Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server - Marked as 'legacy', single server only (Ticket 22484)
Sep 2, 2024	3.0.0	UPDATE - Ensure Soft Delete is Enabled for Azure Containers and Blob Storage - Update Audit/Remediate from CLI and Default Value for accuracy (Ticket 22280)
Sep 2, 2024	3.0.0	UPDATE - Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (CMK) - Update to Rationale explaining Manual Assessment Status (Ticket 22281)
Aug 29, 2024	3.0.0	UPDATE - Ensure that `Allow Blob Anonymous Access` is set to `Disabled` - Consider preview policy to replace the MODIFY policy being currently used. (Ticket 22282)
Aug 9, 2024	3.0.0	UPDATE - Ensure That ‘Users Can Register Applications’ Is Set to ‘No’ - Assessment status changed to Automated (Ticket 21747)
Aug 9, 2024	3.0.0	UPDATE - Ensure That ‘Users Can Register Applications’ Is Set to ‘No’ - Update msol powershell command to mggraph (Ticket 21746)
Sep 2, 2024	3.0.0	UPDATE - Ensure that an exclusionary Geographic Access Policy is considered - Updated Azure AD cmdlets to Graph PowerShell (Ticket 22459)
Aug 26, 2024	3.0.0	UPDATE - Ensure that 'Disk Network Access' is NOT set to 'Enable public access from all networks' - Added CLI & Powershell (Ticket 22413)
Aug 30, 2024	3.0.0	UPDATE - Ensure that 'Endpoint protection' component status is set to 'On' - Title changed, assessment status changed to Automated, prose updated for portal UI changes (Ticket 22417)

Jan 22, 2024	3.0.0	UPDATE - Ensure that Endpoint Protection for all Virtual Machines is installed - Newer policy ID added (Ticket 20579)
Aug 9, 2024	3.0.0	UPDATE - Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users' - Assessment status changed to Automated (Ticket 22307)
Aug 9, 2024	3.0.0	UPDATE - Ensure that 'Guest invite restrictions' is set to 'Only users assigned to specific admin roles can invite guest users' - Powershell audit and remediation procedures added (Ticket 21748)
Aug 9, 2024	3.0.0	UPDATE - Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' - Assessment changed to Automated (Ticket 21749)
Aug 9, 2024	3.0.0	UPDATE - Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' - Powershell updated to use mggraph (Ticket 21750)
Aug 23, 2024	3.0.0	UPDATE - Ensure that 'HTTP20enabled' is set to 'true' (if in use) - Prose updated to reflect 'app' or 'app services', not just 'web app' (Ticket 22273)
Aug 19, 2024	3.0.0	UPDATE - Ensure that 'HTTP20enabled' is set to 'true' (if in use) - Title and Prose updated to reflect the setting name more accurately (Ticket 22379)
Aug 19, 2024	3.0.0	UPDATE - Ensure that 'Java version' is currently supported (if in use) - Changed from 'newest' to 'currently supported' release, updated title and prose (Ticket 22182)

Aug 23, 2024	3.0.0	UPDATE - Ensure that 'Java version' is currently supported (if in use) - Prose updated to reflect 'app' or 'app services', not just 'web app' (Ticket 22272)
Aug 3, 2024	3.0.0	UPDATE - Ensure That Microsoft Defender for Containers Is Set To 'On' - Description updated to highlight Defender for Containers features (Ticket 20486)
Jan 30, 2024	3.0.0	UPDATE - Ensure That Microsoft Defender for Key Vault Is Set To 'On' - Fixed CLI typo (Ticket 19004)
Jan 30, 2024	3.0.0	UPDATE - Ensure That Microsoft Defender for Resource Manager Is Set To 'On' - Fixed CLI typo (Ticket 19006)
Aug 9, 2024	3.0.0	UPDATE - Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users - Correct erroneous change to portal audit steps (Ticket 21073)
Sep 3, 2024	3.0.0	UPDATE - Ensure that Network Security Group Flow logs are captured and sent to Log Analytics - Clarity needed on Description and Audit Procedure - Recommendation updated for clarity (Ticket 17003)
Aug 19, 2024	3.0.0	UPDATE - Ensure that 'PHP version' is currently supported (if in use) - Changed from 'newest' to 'currently supported' release, updated title and prose (Ticket 22382)
Aug 19, 2024	3.0.0	UPDATE - Ensure that 'Python version' is currently supported (if in use) - Changed from 'newest' to 'currently supported' release, updated title and prose (Ticket 22381)

Aug 16, 2024	3.0.0	UPDATE - Ensure that 'Require Multi-Factor Authentication to register or join devices with Microsoft Entra ID' is set to 'Yes' - Added links to CA Policy and updated description and rationale (Ticket 22308)
Aug 9, 2024	3.0.0	UPDATE - Ensure that 'Restrict non-admin users from creating tenants' is set to 'Yes' - Assessment status changed to Automated (Ticket 21745)
Aug 15, 2024	3.0.0	UPDATE - Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) - Syntax correction & addition (Ticket 22060)
Aug 19, 2024	3.0.0	UPDATE - Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults - Permission name corrected to 'List Secret' (Ticket 21899)
Aug 19, 2024	3.0.0	UPDATE - Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults - Permission name corrected to 'List Secret' (Ticket 21898)
Aug 19, 2024	3.0.0	UPDATE - Ensure the Key Vault is Recoverable - Added Azure Policy (Ticket 21395)
Sep 3, 2024	3.0.0	UPDATE - Ensure Trusted Locations Are Defined - Updated Azure AD cmdlets to Graph PowerShell (Ticket 22458)
Aug 28, 2024	3.0.0	UPDATE - Ensure Trusted Locations Are Defined - Updated prose to alert of MFA requirement for Break-Glass Accounts (Ticket 22385)
Aug 29, 2024	3.0.0	UPDATE - Key Vault - Section moved into "Security" parent category section (Ticket 22470)

Aug 30, 2024	3.0.0	UPDATE - Multiple Methods of Audit and Remediation - Information article updated to address Microsoft Graph PowerShell (Ticket 22467)
Sep 2, 2024	3.0.0	UPDATE - Need to review variations between "Single Server" and "Flexible Server" - PostgreSQL recommendations updated to align with flexible server (Ticket 17688)
Sep 3, 2024	3.0.0	UPDATE - Please update Impact to consider new Microsoft best practice - Clarify that Conditional Access should be used instead if possible (Ticket 22141)
Sep 2, 2024	3.0.0	UPDATE - Propose updating the Assessment Status from Manual to Automated - Assessment Status changed from Manual to Automated (Ticket 22439)
Sep 2, 2024	3.0.0	UPDATE - Propose updating the Assessment Status from Manual to Automated - Assessment Status changed from Manual to Automated (Ticket 22442)
Sep 2, 2024	3.0.0	UPDATE - Proposing to update Assessment Status from Manual to Automated for "Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected" - Assessment Status changed from Manual to Automated (Ticket 22416)
Sep 2, 2024	3.0.0	UPDATE - Update Audit from Azure CLI steps, as 'application-insights' CLI extension is GA - Updated Audit CLI steps, command now GA (Ticket 22431)
Sep 2, 2024	3.0.0	UPDATE - Update Audit Procedure to include expected results - Updated audit from CLI command, added expected results for audit (Ticket 22440)

Sep 2, 2024	3.0.0	UPDATE - Update Audit Procedure to include expected results - Updated audit from CLI command, added expected results for audit (Ticket 22441)
Aug 28, 2024 Dec 29, 2023	3.0.0 2.1.0	UPDATE - Use Entra ID Client Authentication and Azure RBAC where possible - Policy added (Ticket 22320) ADD - Ensure fewer than 5 users have global administrator assignment (Ticket 20550)
Feb 13, 2024	2.1.0	ADD - Ensure Multifactor Authentication is Required for Windows Azure Service Management API (Ticket 20670)
Dec 21, 2023	2.1.0	ADD - Ensure only MFA enabled identities can access privileged Virtual Machine (Ticket 19134)
Feb 13, 2024	2.1.0	ADD - Ensure that Microsoft Defender for External Attack Surface Monitoring is enabled (Ticket 20641)
Nov 16, 2023	2.1.0	ADD - Ensure that Private Endpoints are Used for Azure Key Vault - Virtual network service endpoints for Azure Key Vault (Ticket 15428)
Feb 13, 2024	2.1.0	ADD - Ensure Trusted Launch is enabled on Virtual Machines (Ticket 20534)
Jan 9, 2024	2.1.0	ADD - Method Header for Policy - "From Policy" header with applicable policy recommendations added to 100 recommendations (Ticket 15597)
Feb 13, 2024	2.1.0	DELETE - Ensure That Microsoft Defender for Databases Is Set To 'On' - Recommendation was duplicate to other defender recommendations (Ticket 18572)
Dec 27, 2023	2.1.0	DELETE - Ensure that Vulnerability Assessment (VA) is enabled on a SQL server by setting a Storage Account - Vulnerability Assessment no longer need storage configuration (Ticket 17504)
Dec 27, 2023	2.1.0	DELETE - Ensure that Vulnerability Assessment (VA) setting 'Also send email notifications to admins and subscription owners' is set for each SQL Server - Now redundant with Microsoft defender for cloud settings (Ticket 19550)

Feb 13, 2024	2.1.0	DELETE - Ensure that Vulnerability Assessment (VA) setting 'Periodic recurring scans' is set to 'on' for each SQL server - Cannot change periodic scan settings on Defender for SQL (Ticket 19565)
Dec 27, 2023	2.1.0	DELETE - Ensure that Vulnerability Assessment (VA) setting 'Send scan reports to' is configured for a SQL server - Cannot change scan settings on Defender for SQL (Ticket 19567)
Feb 13, 2024	2.1.0	DELETE - Ensure the Storage Container Storing the Activity Logs is not Publicly Accessible - Redundant recommendation (Ticket 18598)
Jan 2, 2024	2.1.0	DELETE - Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' - Remove and move to Compute Services BM (Ticket 19258)
Jan 22, 2024	2.1.0	DELETE - Ensure Access Review is Set Up for External Users in Microsoft Entra ID Privileged Identity Management - Duplicated intent of 1.5 (Ticket 20666)
Dec 21, 2023	2.1.0	UPDATE - Ensure that Network Watcher is 'Enabled' - changes to clarify (Ticket 19013)
Jan 25, 2024	2.1.0	UPDATE - Configuring Diagnostic Settings - Prose to include "Log Analytics" (Ticket 18595)
Dec 21, 2023	2.1.0	UPDATE - Enable Role Based Access Control for Azure Key Vault - Add CLI audit/remediation methods (Ticket 15959)
Jan 30, 2024	2.1.0	UPDATE - Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled - Updated Mitre mapping (Ticket 19963)
Feb 13, 2024	2.1.0	UPDATE - Ensure App Service Authentication is set up for apps in Azure App Service - Added/Updated CLI (Ticket 20539)
Dec 22, 2023	2.1.0	UPDATE - Ensure App Service Authentication is set up for apps in Azure App Service - Additional authentication-related recommendations added (Ticket 17197)
Jan 17, 2024	2.1.0	UPDATE - Ensure Multi-factor Authentication is Required for Risky Sign-ins - Added remediation step to require sign-in frequency every time (Ticket 20663)
Jan 16, 2024	2.1.0	UPDATE - Ensure Multifactor Authentication is Required to access Microsoft Admin Portals - Updated language and procedures for clarity and accuracy (Ticket 17689)

Jan 30, 2024	2.1.0	UPDATE - Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key - Mitre mapping added (Ticket 19415)
Jan 25, 2024	2.1.0	UPDATE - Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests - Portal procedures updated (Ticket 19116)
Jan 25, 2024	2.1.0	UPDATE - Ensure that a 'Diagnostic Setting' exists - Remediation updated to indicate option of 'partner solution' (Ticket 16249)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Network Security Group - Audit procedure for portal updated (Ticket 19047)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Network Security Group - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18912)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Public IP Address rule - Audit procedure for portal updated (Ticket 19053)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Public IP Address rule - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18918)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Security Solution - Audit procedure for portal updated (Ticket 19049)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Security Solution - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18914)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule - Audit procedure for portal updated (Ticket 19051)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18916)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create Policy Assignment - Audit procedure for portal updated (Ticket 19045)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create Policy Assignment - Portal Remediation steps updated (Ticket 18910)

Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Create Policy Assignment - Removed '--location global' from Azure CLI remediation syntax (Ticket 18909)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Network Security Group - Audit procedure for portal updated (Ticket 19048)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Network Security Group - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18913)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Policy Assignment - Audit procedure for portal updated (Ticket 19046)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Policy Assignment - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18911)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Public IP Address rule - Audit procedure for portal updated (Ticket 19054)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Public IP Address rule - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18919)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Security Solution - Audit procedure for portal updated (Ticket 19050)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete Security Solution - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18915)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule - Audit procedure for portal updated (Ticket 19052)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule - Remediation steps updated for portal, and removed '--location global' from CLI syntax (Ticket 18917)
Feb 13, 2024	2.1.0	UPDATE - Ensure That 'All users with the following roles' is set to 'Owner' - Updated CLI Syntax (Ticket 19204)

Jan 22, 2024	2.1.0	UPDATE - Ensure That 'All users with the following roles' is set to 'Owner' - Updated CLI syntax and CLI audit language for accuracy (Ticket 20643)
Dec 28, 2023	2.1.0	UPDATE - Ensure that an exclusionary Geographic Access Policy is considered - Remediation portal steps update (Ticket 16658)
Jan 30, 2024	2.1.0	UPDATE - Ensure that 'Auditing' is set to 'On' - Updated Mitre mapping (Ticket 19418)
Jan 25, 2024	2.1.0	UPDATE - Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On' - CLI Syntax was updated for cleaner output (Ticket 19123)
Feb 13, 2024	2.1.0	UPDATE - Ensure that Auto provisioning of 'Microsoft Defender for Containers components' is Set to 'On' - Procedures Updated (Ticket 17721)
Jan 30, 2024	2.1.0	UPDATE - Ensure that 'Enable key rotation reminders' is enabled for each Storage Account - Added audit and remediation procedures for powershell (Ticket 19490)
Jan 9, 2024	2.1.0	UPDATE - Ensure that Endpoint Protection for all Virtual Machines is installed - Updated Azure CLI query for easier review (Ticket 20551)
Jan 25, 2024	2.1.0	UPDATE - Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks - Audit procedure CLI updated (Ticket 18845)
Jan 26, 2024	2.1.0	UPDATE - Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' - Default value corrected and prose updated with impact detail. (Ticket 19112)
Dec 21, 2023	2.1.0	UPDATE - Ensure that HTTP(S) access from the Internet is evaluated and restricted - include https in audit and remdiation (Ticket 19142)
Jan 30, 2024	2.1.0	UPDATE - Ensure that logging for Azure Key Vault is 'Enabled' - Rationale modified to explain that destination can be Storage Account or Log Analytics workspace (Ticket 19933)
Jan 30, 2024	2.1.0	UPDATE - Ensure that logging for Azure Key Vault is 'Enabled' - Updated CLI, removed retention period with deprecation timeline in additional information (Ticket 19129)

Jan 25, 2024	2.1.0	UPDATE - Ensure that logging for Azure Key Vault is 'Enabled' - Updates to Audit and Remediation Console steps (Ticket 18941)
Jan 30, 2024	2.1.0	UPDATE - Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled' - Clarified description, rationale, and impact regarding "Disabled" policy effect (Ticket 19272)
Jan 30, 2024	2.1.0	UPDATE - Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled' - CLI temporarily removed due to changes (Ticket 19124)
Jan 30, 2024	2.1.0	UPDATE - Ensure that Microsoft Cloud Security Benchmark policies are not set to 'Disabled' - Title and policy initiative naming updated (Ticket 17557)
Jan 30, 2024	2.1.0	UPDATE - Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed' - Updated Mitre mapping (Ticket 19416)
Dec 7, 2023	2.1.0	UPDATE - Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users - wording updates to Audit and Remediation Azure Portal steps (Ticket 16656)
Dec 21, 2023	2.1.0	UPDATE - Ensure that Network Watcher is 'Enabled' - note locations where it wants network watcher to be enabled. (Ticket 17317)
Jan 30, 2024	2.1.0	UPDATE - Ensure That No Custom Subscription Administrator Roles Exist - Removed outdated assignable scope reference (Ticket 19115)
Jan 30, 2024	2.1.0	UPDATE - Ensure That No Custom Subscription Administrator Roles Exist - Updated Mitre mapping (Ticket 19417)
Feb 13, 2024	2.1.0	UPDATE - Ensure That 'PHP version' is the Latest, If Used to Run the Web App - CLI Updated (Ticket 16343)
Jan 25, 2024	2.1.0	UPDATE - Ensure That Private Endpoints Are Used Where Possible - Automation status change from Manual to Automated (Ticket 17324)
Jan 11, 2024	2.1.0	UPDATE - Ensure that 'Public access level' is disabled for storage accounts with blob containers - Added Language for Classic Deployment Model for Storage Accounts (Ticket 20305)
Jan 9, 2024	2.1.0	UPDATE - Ensure that RDP access from the Internet is evaluated and restricted - Blocking source 0.0.0.0 is now included. (Ticket 16169)

Jan 30, 2024	2.1.0	UPDATE - Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) - Automation Status changed from 'Automated' to 'Manual' (Ticket 18775)
May 25, 2023	2.1.0	UPDATE - Ensure that 'Users can create Azure AD Tenants' is set to 'No' - Added Powershell & Changed to Manual Temporarily (Ticket 18493)
Dec 14, 2023	2.1.0	UPDATE - Ensure that 'Users can create Azure AD Tenants' is set to 'No' - Wording change to tile and audit steps (Ticket 18690)
Jan 9, 2024	2.1.0	UPDATE - Ensure the Key Vault is Recoverable - Updated language to indicate soft delete option is deprecated (Ticket 18964)
Jan 25, 2024	2.1.0	UPDATE - Ensure the Storage Container Storing the Activity Logs is not Publicly Accessible - Updated portal/Az CLI/PowerShell Audit Procedures/Remediation Procedures (Ticket 17266)
Jan 25, 2024	2.1.0	UPDATE - Ensure 'TLS Version' is set to 'TLSV1.2' for MySQL flexible Database Server - Included consideration for TLS 1.3 (Ticket 17731)
Dec 21, 2023	2.1.0	UPDATE - Ensure Web App Redirects All HTTP traffic to HTTPS in Azure App Service - change in portal steps for audit and remediation procedure (Ticket 17757)
Jan 22, 2024	2.1.0	UPDATE - Microsoft Defender for Cloud - All MDC recommendations with Policy updated to 'Automated' (Ticket 18241)
Jan 25, 2024	2.1.0	UPDATE - Rename "Azure Active Directory" to "Microsoft Entra ID" everywhere in the document (Ticket 19273)
Feb 14, 2023	2.0.0	UPDATE - Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled - Changed assessment status to automated (Ticket 17695)
Feb 13, 2023	2.0.0	UPDATE - Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' - Removed post-deployment remediation (Ticket 17677)
Feb 13, 2023	2.0.0	UPDATE - Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) - Clarified language in procedure (Ticket 16453)
Feb 13, 2023	2.0.0	UPDATE - Ensure that 'Auditing' Retention is 'greater than 90 days' - Language included to indicate 0 days for unlimited retention (Ticket 17483)

Feb 13, 2023	2.0.0	UPDATE - Ensure that Microsoft Defender for SQL is set to 'On' for critical SQL Servers - Navigation and auditing procedures (Ticket 16452)
Feb 13, 2023	2.0.0	DELETE - Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled' - Duplicate recommendation (Ticket 17471)
Feb 13, 2023	2.0.0	UPDATE - Ensure ‘User consent for applications’ Is Set To ‘Allow for Verified Publishers’ - Updated procedure (Ticket 16261)
Feb 13, 2023	2.0.0	UPDATE - Ensure That 'Notify about alerts with the following severity' is Set to 'High' - Updated default value (Ticket 17370)
Feb 13, 2023	2.0.0	UPDATE - Ensure that ‘Enable Infrastructure Encryption’ for Each Storage Account in Azure Storage is Set to ‘enabled’ - Updated assessment status from Manual to Automated (Ticket 17321)
Feb 13, 2023	2.0.0	UPDATE - Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks - Assessment status updated to automated (Ticket 17323)
Feb 10, 2023	2.0.0	UPDATE - Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) - Updated procedure (Ticket 17655)
Feb 9, 2023	2.0.0	UPDATE - Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On' - Updated steps (Ticket 17645)
Feb 8, 2023	2.0.0	UPDATE - Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults - Updated procedure & language (Ticket 17625)
Feb 8, 2023	2.0.0	UPDATE - Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults - Updated procedure and language (Ticket 17627)
Feb 8, 2023	2.0.0	UPDATE - Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults - Updated procedure and language (Ticket 17630)
Feb 8, 2023	2.0.0	UPDATE - Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults - Updated procedure and language (Ticket 17631)
Jan 31, 2023	2.0.0	UPDATE - Ensure that a 'Diagnostic Setting' exists - Updated the PowerShell/Azure CLI (Ticket 17268)

Jan 31, 2023	2.0.0	UPDATE - Ensure Diagnostic Setting captures appropriate categories - Updated audit/remediation procedures (Ticket 17267)
Jan 31, 2023	2.0.0	UPDATE - Ensure the Storage Container Storing the Activity Logs is not Publicly Accessible - All Audit and Procedure Steps Updated (Ticket 16383)
Jan 31, 2023	2.0.0	UPDATE - Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests - Updated parameter names (Ticket 16937)
Jan 31, 2023	2.0.0	UPDATE - Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests - Updated parameter names (Ticket 16936)
Jan 31, 2023	2.0.0	UPDATE - Ensure That Microsoft Defender for Servers Is Set to 'On' - Updated procedure (Ticket 16675)
Jan 31, 2023	2.0.0	UPDATE - Ensure that Auto provisioning of 'Microsoft Defender for Containers components' is Set to 'On' - Changed from Automated to Manual (Ticket 16597)
Jan 31, 2023	2.0.0	UPDATE - Ensure that 'Users can consent to apps accessing company data on their behalf' is set - Procedure Update and Ordered (Ticket 17109)
Jan 31, 2023	2.0.0	UPDATE - Ensure That ‘Users Can Consent to Apps Accessing Company Data on Their Behalf’ Is Set To ‘Allow for Verified Publishers’ - Updated Procedure (Ticket 16668)
Jan 27, 2023	2.0.0	UPDATE - Ensure That 'PHP version' is the Latest, If Used to Run the Web App - updated CLI (Ticket 17409)
Jan 27, 2023	2.0.0	UPDATE - Ensure that 'Python version' is the Latest Stable Version, if Used to Run the Web App - Add Powershell Audit/Remediation (Ticket 15836)
Jan 27, 2023	2.0.0	UPDATE - Ensure that 'Java version' is the latest, if used to run the Web App - Added detail to AZ CLI & added PowerShell to audit (Ticket 15837)
Jan 27, 2023	2.0.0	UPDATE - Ensure Virtual Machines are utilizing Managed Disks - Changed from Manual to Automated (Ticket 17320)
Jan 27, 2023	2.0.0	UPDATE - Ensure that Network Watcher is 'Enabled' - changed from manual to automated (Ticket 17319)

Jan 27, 2023	2.0.0	UPDATE - Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it - Created Az CLI/PowerShell Audit/Remediation procedures (Ticket 17263)
Jan 27, 2023	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Delete Public IP Address rule - Added Az CLI/PowerShell Audit/remediation procedures (Ticket 17253)
Jan 27, 2023	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Public IP Address rule - Added Az CLI/PowerShell audit/remediation procedures (Ticket 17254)
Jan 27, 2023	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule - Added Az CLI/PowerShell audit/remediation procedures (Ticket 17255)
Jan 27, 2023	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule - Added Az CLI/PowerShell audit/remediation procedures (Ticket 17256)
Jan 27, 2023	2.0.0	UPDATE - Ensure that Activity Log Alert exists for 'Delete Security Rule (Network Security Group)' - type no longer exists (Ticket 15382)
Jan 27, 2023	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Delete Security Solution - Added Az CLI/PowerShell audit/remediation procedures (Ticket 17257)
Jan 27, 2023	2.0.0	DELETE - Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule - type no longer exists (Ticket 15381)
Jan 27, 2023	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Security Solution - Added Az CLI/PowerShell audit/remediation procedures (Ticket 17258)
Jan 27, 2023	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Delete Network Security Group - Added Azure CLI/PowerShell remediation/audit procedures (Ticket 17259)
Jan 27, 2023	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Network Security Group - Added Azure CLI/PowerShell remediation/audit procedures (Ticket 17260)
Jan 27, 2023	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Delete Policy Assignment - Added Az CLI/PowerShell Audit/Remediation procedures (Ticket 17261)
Jan 27, 2023	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Create Policy Assignment - Added Azure CLI/PowerShell audit/remediation back in (Ticket 17262)

Jan 27, 2023	2.0.0	UPDATE - Ensure that logging for Azure AppService 'HTTP logs' is enabled - Log source name updated to current 'HTTP logs' source (Ticket 16689)
Jan 27, 2023	2.0.0	UPDATE - Ensure that logging for Azure Key Vault is 'Enabled' - Updated/added PowerShell and Az CLI to the Audit/Remediation procedures (Ticket 17264)
Jan 27, 2023	2.0.0	UPDATE - Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key - Updated Az CLI and added PowerShell for Audit/remediation procedures (Ticket 17265)
Jan 27, 2023	2.0.0	UPDATE - Ensure Private Endpoints are used to access Storage Accounts - Fix / Add PowerShell & CLI (Ticket 16187)
Jan 27, 2023	2.0.0	UPDATE - Ensure Private Endpoints are used to access Storage Accounts - Assessment status updated to 'automated' (Ticket 17322)
Jan 24, 2023	2.0.0	UPDATE - Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled - Procedure updated (Ticket 16640)
Jan 24, 2023	2.0.0	UPDATE - Ensure that 'Data encryption' is set to 'On' on a SQL Database - Added Powershell Remediation method (Ticket 17473)
Jan 24, 2023	2.0.0	UPDATE - Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server - Added Powershell & updated prose (Ticket 17474)
Jan 24, 2023	2.0.0	UPDATE - Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server - Added Powershell & updated prose (Ticket 17475)
Jan 24, 2023	2.0.0	UPDATE - Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server - Added PowerShell & updated prose (Ticket 17476)
Jan 24, 2023	2.0.0	UPDATE - Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server - Added PowerShell & updated prose (Ticket 17477)
Jan 24, 2023	2.0.0	UPDATE - Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server - Added Powershell & updated prose (Ticket 17478)
Jan 24, 2023	2.0.0	UPDATE - Ensure Server Parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server - Added PowerShell & updated prose (Ticket 17479)

Jan 24, 2023	2.0.0	UPDATE - Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key - Added PowerShell & Updated Prose (Ticket 17480)
Jan 24, 2023	2.0.0	UPDATE - Ensure That 'All users with the following roles' is set to 'Owner' - Prose updated (Ticket 16860)
Jan 24, 2023	2.0.0	UPDATE - Ensure 'Additional email addresses' is Configured with a Security Contact Email - Updated Prose (Ticket 16871)
Jan 24, 2023	2.0.0	UPDATE - Ensure That 'Notify about alerts with the following severity' is Set to 'High' - Updated prose (Ticket 16872)
Jan 24, 2023	2.0.0	UPDATE - Proposed change for Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected - Updated prose (Ticket 16703)
Jan 24, 2023	2.0.0	UPDATE - Ensure that Microsoft Defender for Endpoint integration with Microsoft Defender for Cloud is selected - Remediation procedure correction (Ticket 16702)
Jan 24, 2023	2.0.0	UPDATE - Ensure Any of the ASC Default Policy Settings are Not Set to 'Disabled' - Remediation steps updated for clarity (Ticket 16663)
Jan 20, 2023	2.0.0	ADDED - Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) - New recommendation. (Ticket 17211)
Jan 20, 2023	2.0.0	UPDATE - Ensure That No Custom Subscription Administrator Roles Exist - Extensive update to procedures (Ticket 16737)
Jan 20, 2023	2.0.0	UPDATE - Ensure That Microsoft Defender for Containers Is Set To 'On' - CLI and Powershell syntax (Ticket 16450)
Jan 20, 2023	2.0.0	UPDATE - Ensure That Microsoft Defender for Containers Is Set To 'On' - Procedure steps and product branding updated. (Ticket 16708)
Jan 20, 2023	2.0.0	UPDATE - Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On' - Prose updated for clarity and branding (Ticket 16707)
Jan 20, 2023	2.0.0	UPDATE - Ensure That Microsoft Defender for Key Vault Is Set To 'On' - Prose updated for clarity (Ticket 16706)

Jan 20, 2023	2.0.0	UPDATE - Ensure That Microsoft Defender for DNS Is Set To 'On' - Prose updated for clarity (Ticket 16705)
Jan 20, 2023	2.0.0	UPDATE - Ensure That Microsoft Defender for IoT Hub Is Set To 'On' - Prose and steps updated (Ticket 16451)
Jan 20, 2023	2.0.0	UPDATE - Ensure That Microsoft Defender for Resource Manager Is Set To 'On' - Updated prose for clarity (Ticket 16704)
Jan 19, 2023	2.0.0	UPDATE - Ensure that Resource Locks are set for Mission-Critical Azure Resources - Menu navigation updated (Ticket 16673)
Jan 19, 2023	2.0.0	UPDATE - Enable Role Based Access Control for Azure Key Vault - Navigation and terminology updated (Ticket 16679)
Jan 19, 2023	2.0.0	UPDATE - Ensure that Private Endpoints are Used for Azure Key Vault - Navigation & Terminology (Ticket 16688)
Jan 19, 2023	2.0.0	UPDATE - Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services - Updated terminology (Ticket 16687)
Jan 13, 2023	2.0.0	ADD - External Attack Surface Monitoring - New Section (Ticket 17332)
Dec 27, 2022	2.0.0	UPDATE - Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization - Proposed change to Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization (Ticket 16641)
Dec 27, 2022	2.0.0	UPDATE - Ensure that 'Notify users on password resets?' is set to 'Yes' - Update step 5 (Ticket 16929)
Dec 27, 2022	2.0.0	UPDATE - Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes' - Update step 5 (Ticket 16928)
Dec 23, 2022	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Create Policy Assignment - Improved procedures (Ticket 16909)
Dec 23, 2022	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Delete Policy Assignment - Improved procedures (Ticket 16912)

Dec 23, 2022	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Network Security Group - Improved Procedures (Ticket 16913)
Dec 23, 2022	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Delete Network Security Group - Improved Procedure (Ticket 16914)
Dec 23, 2022	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Security Solution - Improved Procedure (Ticket 16915)
Dec 23, 2022	2.0.0	UPDATE- Ensure that Activity Log Alert exists for Delete Security Solution - Improved procedure (Ticket 16916)
Dec 23, 2022	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule - Improved Procedure (Ticket 16917)
Dec 23, 2022	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule - Improved Procedures (Ticket 16918)
Dec 23, 2022	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Public IP Address rule - Improved Procedure (Ticket 16919)
Dec 23, 2022	2.0.0	UPDATE - Ensure that Activity Log Alert exists for Delete Public IP Address rule - Improved Procedure (Ticket 16920)
Dec 22, 2022	2.0.0	UPDATE - Ensure the Storage Container Storing the Activity Logs is not Publicly Accessible - Improved instructions (Ticket 17004)
Dec 22, 2022	2.0.0	UPDATE - Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key - Improved instructions (Ticket 17006)
Dec 22, 2022	2.0.0	UPDATE - Ensure that logging for Azure Key Vault is 'Enabled' - Improved remediation instructions (Ticket 17056)
Dec 22, 2022	2.0.0	UPDATE - Ensure that Network Security Group Flow logs are captured and sent to Log Analytics - Updated navigation instruction (Ticket 16690)
Dec 14, 2022	2.0.0	UPDATE - Ensure that 'Auditing' is set to 'On' - Updated steps for accuracy (Ticket 17018)

Dec 14, 2022	2.0.0	UPDATE - Ensure that 'Auditing' Retention is 'greater than 90 days' - Prose consistency (Ticket 17020)
Dec 14, 2022	2.0.0	UPDATE - Ensure that Vulnerability Assessment (VA) setting 'Send scan reports to' is configured for a SQL server - Updated procedure (Ticket 16695)
Dec 14, 2022	2.0.0	UPDATE - Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled - Procedure Updated (Ticket 16667)
Dec 14, 2022	2.0.0	UPDATE - Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server - Procedure Improved (Ticket 16678)
Dec 14, 2022	2.0.0	UPDATE - Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server - Procedure Improved (Ticket 16701)
Dec 14, 2022	2.0.0	UPDATE - Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks - Procedure updated (Ticket 16700)
Dec 14, 2022	2.0.0	UPDATE - Ensure That Private Endpoints Are Used Where Possible - Procedure Updated (Ticket 16693)
Dec 7, 2022	2.0.0	UPDATE - Ensure that ‘Enable Infrastructure Encryption’ for Each Storage Account in Azure Storage is Set to ‘enabled’ - Navigation Corrections (Ticket 16677)
Dec 7, 2022	2.0.0	UPDATE - Ensure that 'Enable key rotation reminders' is enabled for each Storage Account - Steps updated (Ticket 16664)
Dec 6, 2022	2.0.0	UPDATE - Ensure that Auto provisioning of 'Vulnerability assessment for machines' is Set to 'On' - Change to Manual assessment (Ticket 16596)
Nov 30, 2022	2.0.0	UPDATE - Ensure That Microsoft Defender for App Services Is Set To 'On' - Menu Navigation Update (Ticket 16672)
Nov 30, 2022	2.0.0	UPDATE - Ensure That Microsoft Defender for Databases Is Set To 'On' - Navigation Updated (Ticket 16676)
Nov 16, 2022	2.0.0	UPDATE - Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization - (Ticket 16931)

Nov 16, 2022	2.0.0	UPDATE - Ensure that 'Require Multi-Factor Authentication to register or join devices with Azure AD' is set to 'Yes' - update step 2 (Ticket 16932)
Nov 7, 2022	2.0.0	UPDATE - Minor format error in Audit Procedure (Ticket 16287)
Sep 7, 2022	2.0.0	UPDATE - CLI/API Availability - Review all "At this point of time" statements (Ticket 16224)
Aug 26, 2022	2.0.0	UPDATE - Ensure that logging for Azure AppService 'AppServiceHTTPLogs' is enabled. - Ensure that "AppServiceHTTPLogs" is set to "Enabled" (Ticket 15892)
Aug 26, 2022	2.0.0	UPDATE - 2.3.1 Ensure That 'All users with the following roles' is set to 'Owner' - Fix typo in 2.3.1 Audit and Remediation Procedure (Ticket 16257)
Aug 25, 2022	2.0.0	UPDATE - Section 5 - 'Security' is misspelled in 5.2.3, 5.2.4, 5.2.5, 5.2.6 (Ticket 16251)
Aug 23, 2022	2.0.0	UPDATE - Ensure Soft Delete is Enabled for Azure Containers and Blob Storage - Remove errant '>' in 3.11 Remediation Procedure (Ticket 16256)
Aug 23, 2022	2.0.0	UPDATE - Enable Role Based Access Control for Azure Key Vault - Typo in 8.6 Remediation Procedure (Ticket 16252)
Aug 23, 2022	2.0.0	UPDATE - Ensure that Vulnerability Assessment (VA) setting 'Also send email notifications to admins and subscription owners' is set for each SQL Server - Update numbering in 4.2.5 Remediation Procedure (Ticket 16254)
Aug 23, 2022	2.0.0	UPDATE - Ensure that 'Guest invite restrictions' is set to "Only users assigned to specific admin roles can invite guest users" - Typo in 1.16 Remediation Procedure (Ticket 16253)