CIS Benchmarks

CIS Microsoft Azure Foundations Benchmark

v1.3.1 - 07-21-2021

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/

Table of Contents

Overview

This document, CIS Microsoft Azure Foundations Security 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. The benchmark is, however, not an exhaustive list of all possible security configurations and architecture. You should take the benchmark as a starting point and do the required site-specific tailoring wherever needed and when it is prudent to do so.
To obtain the latest version of this guide, please visit https://www.cisecurity.org/cis-benchmarks/. 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 benchmark was created using a consensus review process comprised of subject matter experts. 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, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

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 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
Gururaj Pandurangi
Ben Layer
Felix Simmons
Jonathan Trull
Pravin Goyal
Pradeep R B
Prabhu Angadi
Robin Drake
Shobha H D
Rahul Khengare
Jesse Mrasek
Kesten Broughton
Himalay Kondekar
JR Aquino
Jeremie Kass
Sujit Singh
Robert Burton
Clément Bonnet
Lewis Matlock
Clifford Moten
Mike Wicks
Sean Decker
Phil White
Ronit Reger
Jim Cheng

Editor
Parag Patil
Iben Rodriguez

Recommendations

1 Identity and Access Management

This section covers security recommendations that to follow to set identity and access management policies on an Azure Subscription. Identity and Access Management policies are the first step towards a defense-in-depth approach to securing an Azure Cloud Platform environment.

Most of the recommendations from this section are marked as "Not Scored" because of the lack of "Azure native CLI and API support" to perform the respective audits. However, from a security posture standpoint, these recommendations are important. According to the last communication with the Microsoft Support team regarding "Azure native CLI and API support", Microsoft teams are working to enhance "Microsoft graph API" to support all these "Azure AD" functionalities. Once we get this capability through "Microsoft Graph API", we will update the involved recommendations with the respective audit and remediation steps to make them as scored.

1.1 Ensure that multi-factor authentication is enabled for all privileged users (Manual)

Profile Applicability:

- Level 1

Description:

Enable multi-factor authentication for all user credentials who have write access to Azure resources. These include roles like

- 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 action is granted. Also, this requires an overhead for managing dual forms of authentication.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `All Users`
4. Click on `Multi-Factor Authentication` button on the top bar
5. Ensure that `MULTI-FACTOR AUTH STATUS` is `Enabled` for all users who are `Service Co-Administrators` OR `Owners` OR `Contributors`.

Microsoft Graph 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 MSOL Powershell command:

```
Get-MsolUser -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.
Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation. Only option is MSOL

Remediation:

Follow Microsoft Azure documentation and setup multi-factor authentication in your environment.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access

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.		●	●

1.2 Ensure that multi-factor authentication is enabled for all non-privileged users (Manual)

Profile Applicability:

- Level 2

Description:

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 action is granted. Also, this requires an overhead for managing dual forms of authentication.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `All Users`
4. Click on `Multi-Factor Authentication` button on the top bar
5. Ensure that for all users `MULTI-FACTOR AUTH STATUS` is `Enabled`

Microsoft Graph 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/Microsoft.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/Microsoft.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 MSOL Powershell command:

```
Get-MsolUser -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.
Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation. Only option is MSOL

Remediation:

Follow Microsoft Azure documentation and setup multi-factor authentication in your environment.
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa

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://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access

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.		●	●

1.3 Ensure guest users are reviewed on a monthly basis (Automated)

Profile Applicability:

- Level 1

Description:

Azure AD is extended to include Azure AD B2B collaboration, 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. Guest users allow you to share your company's applications and services with users from any other organization, while maintaining control over your own corporate data.

Work with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources a a guest user.

Rationale:

Guest users in the Azure AD are generally required for collaboration purposes in Office 365, and may also be required for Azure functions in enterprises with multiple Azure tenants, Guest users should be reviewed on a regular basis, at least annually, Guest users should not be granted administrative roles where possible.

Guest users are typically added outside your employee on-boarding/off-boarding process and could potentially be overlooked indefinitely leading to a potential vulnerability.

Guest users should be review on a monthly basis to ensure that inactive and unneeded accounts are removed.

Impact:

Until you have a business need to provide guest access to any user, avoid creating guest users. If guest accounts are being used, they should be removed when no longer required.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `All Users`
4. Click on `Show` drop down and select `Guest users only`

5. Ensure that guest users listed are still required (`USER TYPE` = `Guest`)

Using Azure Command Line Interface 2.0

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

Ensure all users listed are not inactive and still required.

Using PowerShell

```
Connect-AzureAD   (Only needs to be performed once within the PowerShell
session)
Get-AzureADUser |Where-Object {$_.UserType -like "Guest"} |Select-Object
DisplayName, UserPrincipalName, UserType -Unique
```

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users and group`
3. Go to `All Users`
4. Click on `Show` drop down and select `Guest users only`
5. Delete all "Guest" users that are no longer required or are inactive.

It is good practice to use a dynamic group to manage guest users.
To create the dynamic group:

1. Navigate to the `Active Directory` 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.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/b2b/user-properties
2. https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory#delete-a-user
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-3-review-and-reconcile-user-access-regularly

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●
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	16.8 Disable Any Unassociated Accounts Disable any account that cannot be associated with a business process or business owner.	●	●	●

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

Profile Applicability:

- Level 2

Description:

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 by-pass 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:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `All Users`
4. Click on `Multi-Factor Authentication` 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

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`

2. Go to `Users`
3. Go to `All Users`
4. Click on `Multi-Factor Authentication` button on the top bar
5. Click on `service settings`
6. Disable `Allow users to remember multi-factor authentication on devices they trust`

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication-whats-next#remember-multi-factor-authentication-for-devices-that-users-trust
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access

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.		●	●

1.5 Ensure that 'Number of methods required to reset' is set to '2' (Manual)

Profile Applicability:

- Level 1

Description:

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

Rationale:

Like multi-factor authentication, setting up dual identification before allowing a password reset ensures that the user identity is confirmed via two separate forms of identification. With dual identification set, an attacker would require compromising both the identity forms before he/she could maliciously reset a user's password.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `Password reset`
4. Go to `Authentication methods`
5. Ensure that `Number of methods required to reset` is set to `2`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `Password reset`
4. Go to `Authentication methods`
5. Set the `Number of methods required to reset` to `2`

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-faq#password-reset-registration
2. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access

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.		●	●

1.6 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:

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, such as a phone number or email changes, then the password reset information for that user reverts to the previously registered authentication information.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `Password reset`
4. Go to `Registration`
5. Ensure that `Number of days before users are asked to re-confirm their authentication information` is not set to `0`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `Password reset`
4. Go to `Registration`
5. Set the `Number of days before users are asked to re-confirm their authentication information` to your organization defined frequency

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://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-how-it-works#registration
2. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-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 Account Monitoring and Control Account Monitoring and Control			

1.7 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 secondary emails on password resets.

Rationale:

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

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `Password reset`
4. Go to `Notification`
5. Ensure that `Notify users on password resets?` is set to `Yes`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `Password reset`
4. Go to `Notification`
5. Set `Notify users on password resets?` to `Yes`

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-how-it-works#notifications
2. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-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 Account Monitoring and Control Account Monitoring and Control			

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

Profile Applicability:

- Level 2

Description:

Ensure that all 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 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.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `Password reset`
4. Go to `Notification`
5. Ensure that `notify all admins when other admins reset their password?` is set to `Yes`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `Password reset`
4. Go to `Notification`
5. Set `Notify all admins when other admins reset their password?` to `Yes`

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-how-it-works#notifications
2. https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-identity-and-privileged-access-strategy
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-2-restrict-administrative-access-to-business-critical-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.	●	●	●
v7	4 Controlled Use of Administrative Privileges Controlled Use of Administrative Privileges			

1.9 Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No' (Manual)

Profile Applicability:

- Level 2

Description:

Require administrators to provide consent for the apps before use.

Rationale:

Unless Azure Active Directory is running as an identity provider for third-party applications, do not allow users to use their identity outside of the cloud environment. User profiles contain private information such as phone numbers and email addresses which could then be sold off to other third parties without requiring any further consent from the user.

Impact:

It might be an additional request that administrators need to fulfill quite often.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `User settings`
4. Click on `Manage how end users launch and view their applications`
5. Ensure that `Users can consent to apps accessing company data on their behalf` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Using PowerShell

```
Connect-MsolService
Get-MsolCompanyInformation | Select-Object
UsersPermissionToUserConsentToAppEnabled
```

Command should return `UsersPermissionToUserConsentToAppEnabled` with the value of `False`

Remediation:

Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `User settings`
4. Click on `Manage how end users launch and view their applications`
5. Set `Users can consent to apps accessing company data on their behalf` to `No`

Default Value:

By default, 'Users can consent to apps accessing company data on their behalf' is set to 'Yes'.

References:

1. https://blogs.msdn.microsoft.com/exchangedev/2014/06/05/managing-user-consent-for-applications-using-office-365-apis/
2. https://nicksnettravels.builttoroam.com/post/2017/01/24/Admin-Consent-for-Permissions-in-Azure-Active-Directory.aspx
3. https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent#configure-user-consent-to-applications
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems
6. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
7. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-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 Account Monitoring and Control Account Monitoring and Control			

1.10 Ensure that 'Users can add gallery apps to their Access Panel' is set to 'No' (Manual)

Profile Applicability:

- Level 2

Description:

Require administrators to provide consent for the apps before use.

Rationale:

Unless Azure Active Directory is running as an identity provider for third-party applications, do not allow users to use their identity outside of your cloud environment. User profiles contain private information such as phone numbers and email addresses which could then be sold off to other third parties without requiring any further consent from the user.

Impact:

It might be an additional request that administrators need to fulfill quite often.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `User settings`
4. Click on `Manage how end users launch and view their applications`
5. Ensure that `Users can add gallery apps to their Access Panel` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `User settings`
4. Click on `Manage how end users launch and view their applications`

5. Set `Users can add gallery apps to their Access Panel` to `No`

Default Value:

By default, 'Users can add gallery apps to their Access Panel' is set to 'No'.

References:

1. https://blogs.msdn.microsoft.com/exchangedev/2014/06/05/managing-user-consent-for-applications-using-office-365-apis/
2. https://nicksnettravels.builttoroam.com/post/2017/01/24/Admin-Consent-for-Permissions-in-Azure-Active-Directory.aspx
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-1-define-asset-management-and-data-protection-strategy
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●
v7	2 Inventory and Control of Software Assets Inventory and Control of Software Assets			

1.11 Ensure that 'Users can register applications' is set to 'No' (Manual)

Profile Applicability:

- Level 2

Description:

Require administrators to register third-party applications.

Rationale:

It is recommended to let administrator register custom-developed applications. This ensures that the application undergoes a security review before exposing active directory data to it.

Impact:

This might create additional requests that administrators need to fulfill quite often.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `User settings`
4. Ensure that `Users can register applications` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.
Using PowerShell

```
Connect-MsolService
Get-MsolCompanyInformation | Select-Object
UsersPermissionToCreateLOBAppsEnabled
```

Command should return `UsersPermissionToCreateLOBAppsEnabled` with the value of `False`

Remediation:

From Azure Console

1. Go to `Azure Active Directory`

2. Go to `Users`
3. Go to `User settings`
4. Set `Users can register applications` to `No`

Default Value:

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

References:

1. https://blogs.msdn.microsoft.com/exchangedev/2014/06/05/managing-user-consent-for-applications-using-office-365-apis/
2. https://nicksnettravels.builttoroam.com/post/2017/01/24/Admin-Consent-for-Permissions-in-Azure-Active-Directory.aspx
3. https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added#who-has-permission-to-add-applications-to-my-azure-ad-instance
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-1-define-asset-management-and-data-protection-strategy
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
6. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
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.		●	●
v7	2 Inventory and Control of Software Assets Inventory and Control of Software Assets			

1.12 Ensure that 'Guest user permissions are limited' is set to 'Yes' (Manual)

Profile Applicability:

- Level 2

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. If guest access in not limited, they have the same access to directory data as regular users.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `External Identities`
3. Go to `External collaboration settings`
4. Ensure that `Guest users permissions are limited` is set to `Yes`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `External Identities`
3. Go to `External collaboration settings`
4. Set `Guest users permissions are limited` to `Yes`

Default Value:

By default, `Guest users permissions are limited` is set to `Yes`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions#member-and-guest-users
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-5-automate-entitlement-management
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-identity-and-privileged-access-strategy

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	16 Account Monitoring and Control Account Monitoring and Control			

1.13 Ensure that 'Members can invite' is set to 'No' (Manual)

Profile Applicability:

- Level 2

Description:

Restrict invitations to administrators only.

Rationale:

Restricting invitations to administrators 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 `Admins and users in the guest inviter role can invite` is set to yes. This will allow you to use the `inviter` role to control who will be able to invite guests to the tenant.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `External Identities`
3. Go to `External collaboration settings`
4. Ensure that `Members can invite` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `External Identities`
3. Go to `External collaboration settings`
4. Set `Members can invite` to `No`

Default Value:

By default, `Members can invite` is set to `Yes`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-delegate-invitations
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-identity-and-privileged-access-strategy
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-5-automate-entitlement-management

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	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			
v7	16 Account Monitoring and Control Account Monitoring and Control			

1.14 Ensure that 'Guests can invite' is set to 'No' (Manual)

Profile Applicability:

- Level 2

Description:

Restrict guest being able to invite other guests to collaborate with your organization.

Rationale:

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

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `External Identities`
3. Go to `External collaboration settings`
4. Ensure that `Guests can invite` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `External Identities`
3. Go to `External collaboration settings`
4. Set `Guests can invite` to `No`

Default Value:

By default, `Guests can invite` is set to `Yes`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-delegate-invitations

2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-5-automate-entitlement-management
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
6. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-identity-and-privileged-access-strategy

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	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			
v7	16 Account Monitoring and Control Account Monitoring and Control			

1.15 Ensure that 'Restrict access to Azure AD administration portal' is set to 'Yes' (Manual)

Profile Applicability:

- Level 1

Description:

Restrict access to the Azure AD administration portal to administrators only.

Rationale:

The Azure AD administrative portal has sensitive data. All non-administrators should be prohibited from accessing any Azure AD data in the administration portal to avoid exposure.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `User settings`
4. Ensure that `Restrict access to Azure AD administration portal` is set to `Yes`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Users`
3. Go to `User settings`
4. Set `Restrict access to Azure AD administration portal` to `Yes`

Default Value:

By default, `Restrict access to Azure AD administration portal` is set to `No`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-assign-admin-roles-azure-portal
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-identity-and-privileged-access-strategy
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems

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	4 Controlled Use of Administrative Privileges Controlled Use of Administrative Privileges			
v7	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			

1.16 Ensure that 'Restrict user ability to access groups features in the Access Pane' is set to 'No' (Manual)

Profile Applicability:

- Level 2

Description:

Restrict group creation to administrators only.

Rationale:

Self-service group management enables users to create and manage security groups or Office 365 groups in Azure Active Directory (Azure AD). Unless a business requires this day-to-day delegation for some users, self-service group management should be disabled.

Impact:

Enabling this setting could create a number of request that would need to me managed by administrators.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Groups`
3. Go to `General` in setting
4. Ensure that `Restrict user ability to access groups features in the Access Pane` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Groups`
3. Go to `General` in setting
4. Ensure that `Restrict user ability to access groups features in the Access Pane` is set to `No`

Default Value:

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

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-self-service-group-management
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-5-automate-entitlement-management
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
6. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-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	16 Account Monitoring and Control Account Monitoring and Control			

1.17 Ensure that 'Users can create security groups in Azure Portals' 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 request that would need to be managed by an administrator.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Groups`
3. Go to `General` in setting
4. Ensure that `Users can create security groups in Azure Portals` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Groups`
3. Go to `General` in setting
4. Set `Users can create security groups in Azure Portals` to `No`

Default Value:

By default, `Users can create security groups` is set to `Yes`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-self-service-group-management#making-a-group-available-for-end-user-self-service
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-identity-and-privileged-access-strategy
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-5-automate-entitlement-management
6. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems

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	16 Account Monitoring and Control Account Monitoring and Control			

1.18 Ensure that 'Owners can manage group membership requests in the Access Panel' 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.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Groups`
3. Go to `General` in settings
4. Ensure that `Owners can manage group membership requests in the Access Panel` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Groups`
3. Go to `General` in settings
4. Set `Owners can manage group membership requests in the Access Panel' to No`

Default Value:

By default, `Owners can manage group membership requests in the Access Panel` is set to `No`.

References:

1. https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-self-service-group-management#making-a-group-available-for-end-user-self-service
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-5-automate-entitlement-management
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-8-choose-approval-process-for-microsoft-support
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
6. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-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	16 Account Monitoring and Control Account Monitoring and Control			

1.19 Ensure that 'Users can create Microsoft 365 groups in Azure Portals' 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 request that would need to be managed by an administrator.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Groups`
3. Go to `General` in setting
4. Ensure that `Users can create Microsoft 365 groups in Azure Portals` is set to `No`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Groups`
3. Go to `General` in setting
4. Set `Users can create Microsoft 365 groups in Azure Portals` to `No`

Default Value:

By default, `Users can create Microsoft 365 groups in Azure Portals` is set to `Yes`.

References:

1. https://whitepages.unlimitedviz.com/2017/01/disable-office-365-groups-2/
2. https://support.office.com/en-us/article/Control-who-can-create-Office-365-Groups-4c46c8cb-17d0-44b5-9776-005fced8e618
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-identity-and-privileged-access-strategy
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
6. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-5-automate-entitlement-management
7. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems

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	16 Account Monitoring and Control Account Monitoring and Control			

1.20 Ensure that 'Require Multi-Factor Auth to join devices' is set to 'Yes' (Manual)

Profile Applicability:

- Level 1

Description:

Joining devices to the active directory should require Multi-factor authentication.

Rationale:

Multi-factor authentication is recommended when adding devices to Azure AD. 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 directory for a compromised user account.

Audit:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Devices`
3. Go to `Device settings`
4. Ensure that `Require Multi-Factor Auth to join devices` is set to `Yes`

Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

Remediation:

From Azure Console

1. Go to `Azure Active Directory`
2. Go to `Devices`
3. Go to `Device settings`
4. Set `Require Multi-Factor Auth to join devices` to `Yes`

Default Value:

By default, `Require Multi-Factor Auth to join devices` is set to `No`.

References:

1. https://blogs.technet.microsoft.com/janketil/2016/02/29/azure-mfa-for-enrollment-in-intune-and-azure-ad-device-registration-explained/
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access

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.		●	●
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.		●	●

1.21 Ensure that no custom subscription owner roles are created (Automated)

Profile Applicability:

- Level 2

Description:

Subscription ownership should not include permission to create custom owner roles. The principle of least privilege should be followed and only necessary privileges should be assigned instead of allowing full administrative access.

Rationale:

Classic subscription admin roles offer basic access management and include Account Administrator, Service Administrator, and Co-Administrators. It is recommended the least necessary permissions be given initially. Permissions can be added as needed by the account holder. This ensures the account holder cannot perform actions which were not intended.

Audit:

Using Azure Command Line Interface 2.0

```
az role definition list
```

Check for entries with `assignableScope` of `/` or a `subscription`, and an action of `*`
Verify the usage and impact of removing the role identified
Using PowerShell

```
Connect-AzAccount
Get-AzRoleDefinition |Where-Object {($.IsCustom -eq $true) -and ($.Name -like
"Owner")}
```

Review output for each returned role's 'AssignableScopes' value for '/' or the current subscription, and 'Actions' containing the '*' wildcard character.

Remediation:

Using Azure Command Line Interface 2.0

```
az role definition list
```

Check for entries with `assignableScope` of `/` or a `subscription`, and an action of `*`
Verify the usage and impact of removing the role identified

```
az role definition delete --name "rolename"
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-identity-and-privileged-access-strategy
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-5-automate-entitlement-management
6. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems
7. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
8. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-identity-and-privileged-access-strategy
9. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-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.	●	●	●
v7	4 Controlled Use of Administrative Privileges Controlled Use of Administrative Privileges			

Controls Version	Control	IG 1	IG 2	IG 3
v7	16 Account Monitoring and Control Account Monitoring and Control			

1.22 Ensure Security Defaults is enabled on Azure Active Directory (Automated)

Profile Applicability:

- Level 1

Description:

Security defaults in Azure Active Directory (Azure AD) make it easier to be secure and help protect your organization. Security defaults contain preconfigured security settings for common attacks.

Microsoft is making security defaults available to everyone. The goal is to ensure that all organizations have a basic level of security-enabled at no extra cost. You 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 - mostly when they show up on a new device or app, but more often for critical roles and tasks.
- Disabling authentication from legacy authentication clients, which can't do MFA.

Impact:

Enabling security defaults may negatively impact the functionality of other Microsoft services, such as MS365. This recommendation should be implemented initially and then may be overridden by other service/product specific CIS Benchmarks.

Audit:

From Azure Console
To ensure security defaults is enabled in your directory:

1. Sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator.
2. Browse to Azure Active Directory > Properties.
3. Select Manage security defaults.

4. Verify the Enable security defaults toggle to Yes.

Remediation:

From Azure Console
To enable security defaults in your directory:

1. Sign in to the Azure portal as a security administrator, Conditional Access administrator, or global administrator.
2. Browse to Azure Active Directory > Properties.
3. Select Manage security defaults.
4. Set the Enable security defaults toggle to Yes.
5. Select Save.

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

Additional Information:

The setting in this recommendation are different in the Microsoft 365 Benchmark. This is because the potential impact associated with disabling of Security Defaults is dependent upon the security settings implemented in the environment. It is recommended that organizations disabling Security Defaults plan to implement equivalent 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.	●	●	●
v7	13 Data Protection Data Protection			

1.23 Ensure Custom Role is assigned 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 is you can have specific permissions granted for managing just resource locks rather than needing to provide the wide owner or contributor role reducing the risk of the user being able to do unintentional damage.

Audit:

From Azure Console

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

Remediation:

From Azure Console

1. In the Azure portal, open a subscription or resource group where you want the custom role to be assignable.
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. Click `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. Select the check box next to the permission called `Microsoft.Authorization/locks`
12. click `add`
13. Click `Review+create`
14. Click `Create`

Assign the newly created role to the appropriate user.

Using 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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems

5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-7-follow-just-enough-administration-least-privilege-principle
6. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-5-automate-entitlement-management
7. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
8. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-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.	●	●	●
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 Security Center

This section covers security recommendations to follow when setting various security policies on an Azure Subscription. A security policy defines the set of controls, which are recommended for resources within the specified Azure subscription. Please note that the majority of the recommendations mentioned in this section only produce an alert if a security violation is found. They do not actually enforce security settings by themselves. Alerts should be acted upon and remedied wherever possible.

2.1 Ensure that Azure Defender is set to On for Servers (Manual)

Profile Applicability:

- Level 2

Description:

Turning on Azure Defender enables threat detection for Server, providing threat intelligence, anomaly detection, and behavior analytics in the Azure Security Center.

Rationale:

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

Impact:

Turning on Azure Defender in Azure Security Center incurs an additional cost per resource.

Audit:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. Review the chosen pricing tier. For the `Servers` resource type `Plan` should be set to `On`.

Using Azure Command Line Interface 2.0
Ensure the output of the below command is Standard

```
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/pr
icings?api-version=2018-06-01' | jq '.|.value[] |
select(.name=="VirtualMachines")'|jq '.properties.pricingTier'
```

Using PowerShell

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

Ensure output of command is `VirtualMachines Standard`

Remediation:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. On the line in the table for `Servers` Select `On` under `Plan`.
6. Select `Save`

Using Azure Command Line Interface 2.0

Use the below command to enable Azure Defender for Servers

```
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/pr
icings/VirtualMachines?api-version=2018-06-01 -d@"input.json"'
```

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

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/pricings/
VirtualMachines",
  "name": "VirtualMachines",
  "type": "Microsoft.Security/pricings",
  "properties": {
    "pricingTier": "Standard"
  }
}
```

Default Value:

By default, Azure Defender off is selected.

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-endpoint-security#es-1-use-endpoint-detection-and-response-edr

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

2.2 Ensure that Azure Defender is set to On for App Service (Manual)

Profile Applicability:

- Level 2

Description:

Turning on Azure Defender enables threat detection for App Service, providing threat intelligence, anomaly detection, and behavior analytics in the Azure Security Center.

Rationale:

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

Impact:

Turning on Azure Defender in Azure Security Center incurs an additional cost per resource.

Audit:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. Review the chosen pricing tier. For the `App Service` resource type `Plan` should be set to `On`.

Using Azure Command Line Interface 2.0
Ensure the output of the below command is Standard

```
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/pr
icings?api-version=2018-06-01' | jq '.|.value[] |
select(.name=="AppServices")'|jq '.properties.pricingTier'
```

Using PowerShell

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

Ensure output of `Name PricingTier` is `AppServices Standard`

Remediation:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. On the line in the table for `App Service` Select `On` under `Plan`.
6. Select `Save

Using Azure Command Line Interface 2.0
Use the below command to enable Standard pricing tier for App Service

```
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/pr
icings/AppServices?api-version=2018-06-01 -d@"input.json"'
```

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

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/pricings/
AppServices",
  "name": "AppServices",
  "type": "Microsoft.Security/pricings",
  "properties": {
    "pricingTier": "Standard"
  }
}
```

Default Value:

By default, Azure Defender off is selected.

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

2.3 Ensure that Azure Defender is set to On for Azure SQL database servers (Manual)

Profile Applicability:

- Level 2

Description:

Turning on Azure Defender enables threat detection for Azure SQL database servers, providing threat intelligence, anomaly detection, and behavior analytics in the Azure Security Center.

Rationale:

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

Impact:

Turning on Azure Defender in Azure Security Center incurs an additional cost per resource.

Audit:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. Review the chosen pricing tier. For the `Azure SQL database servers` resource type `Plan` should be set to `On`.

Using Azure Command Line Interface 2.0
Ensure the output of the below command is Standard

```
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/pr
icings?api-version=2018-06-01' | jq '.|.value[] |
select(.name=="SqlServers")'|jq '.properties.pricingTier'
```

Using PowerShell

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

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

Remediation:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. On the line in the table for `Azure SQL database servers` Select `On` under `Plan`.
6. Select `Save`

Using Azure Command Line Interface 2.0

Use the below command to enable Standard pricing tier for Azure SQL database servers

```
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/pr
icings/SqlServers?api-version=2018-06-01 -d@"input.json"'
```

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

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/pricings/
SqlServers",
  "name": "SqlServers",
  "type": "Microsoft.Security/pricings",
  "properties": {
    "pricingTier": "Standard"
  }
}
```

Default Value:

By default, Azure Defender off is selected.

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-3-monitor-for-unauthorized-transfer-of-sensitive-data

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

2.4 Ensure that Azure Defender is set to On for SQL servers on machines (Manual)

Profile Applicability:

- Level 2

Description:

Turning on Azure Defender enables threat detection for SQL servers on machines, providing threat intelligence, anomaly detection, and behavior analytics in the Azure Security Center.

Rationale:

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

Impact:

Turning on Azure Defender in Azure Security Center incurs an additional cost per resource.

Audit:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. Review the chosen pricing tier. For the `SQL Servers on machines` resource type `Plan` should be set to `On`.

Using Azure Command Line Interface 2.0
Ensure the output of the below command is Standard

```
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/pr
icings?api-version=2018-06-01' | jq '.|.value[] |
select(.name=="SqlserverVirtualMachines")'|jq '.properties.pricingTier'
```

Using PowerShell

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

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

Remediation:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. On the line in the table for `SQL Servers on machines` Select `On` under `Plan`.
6. Select `Save`

Using Azure Command Line Interface 2.0

Use the below command to enable Standard pricing tier for Storage

```
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/pr
icings/StorageAccounts?api-version=2018-06-01 -d@"input.json"'
```

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

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/pricings/
StorageAccounts",
  "name": "StorageAccounts",
  "type": "Microsoft.Security/pricings",
  "properties": {
    "SqlserverVirtualMachines": "Standard"
  }
}
```

Default Value:

By default, Azure Defender off is selected.

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-3-monitor-for-unauthorized-transfer-of-sensitive-data

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

2.5 Ensure that Azure Defender is set to On for Storage (Manual)

Profile Applicability:

- Level 2

Description:

Turning on Azure Defender enables threat detection for Storage, providing threat intelligence, anomaly detection, and behavior analytics in the Azure Security Center.

Rationale:

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

Impact:

Turning on Azure Defender in Azure Security Center incurs an additional cost per resource.

Audit:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. Review the chosen pricing tier. For the `Storage` resource type `Plan` should be set to `On`.

Using Azure Command Line Interface 2.0
Ensure the output of the below command is Standard

```
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/pr
icings?api-version=2018-06-01' | jq '.|.value[] |
select(.name=="StorageAccounts")'|jq '.properties.pricingTier'
```

Using PowerShell

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

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

Remediation:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. On the line in the table for `Storage` Select `On` under `Plan`.
6. Select `Save`

Using Azure Command Line Interface 2.0

Use the below command to enable Standard pricing tier for Storage

```
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/pr
icings/StorageAccounts?api-version=2018-06-01 -d@"input.json"'
```

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

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/pricings/
StorageAccounts",
  "name": "StorageAccounts",
  "type": "Microsoft.Security/pricings",
  "properties": {
    "pricingTier": "Standard"
  }
}
```

Default Value:

By default, Azure Defender off is selected.

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-endpoint-security#es-1-use-endpoint-detection-and-response-edr

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

2.6 Ensure that Azure Defender is set to On for Kubernetes (Manual)

Profile Applicability:

- Level 2

Description:

Turning on Azure Defender enables threat detection for Kubernetes, providing threat intelligence, anomaly detection, and behavior analytics in the Azure Security Center.

Rationale:

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

Impact:

Turning on Azure Defender in Azure Security Center incurs an additional cost per resource.

Audit:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. Review the chosen pricing tier. For the `Kubernetes` resource type `Plan` should be set to `On`.

Using Azure Command Line Interface 2.0
Ensure the output of the below command is Standard

```
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/pr
icings?api-version=2018-06-01' | jq '.|.value[] |
select(.name=="KubernetesService")'|jq '.properties.pricingTier'
```

Using PowerShell

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

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

Remediation:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. On the line in the table for `Kubernetes` Select `On` under `Plan`.
6. Select `Save`

Using Azure Command Line Interface 2.0

Use the below command to enable Standard pricing tier for Storage

```
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/pr
icings/StorageAccounts?api-version=2018-06-01 -d@"input.json"'
```

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

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/pricings/
StorageAccounts",
  "name": "KubernetesService",
  "type": "Microsoft.Security/pricings",
  "properties": {
    "pricingTier": "Standard"
  }
}
```

Default Value:

By default, Azure Defender off is selected.

References:

1. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list
2. https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update
3. https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities
4. https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

2.7 Ensure that Azure Defender is set to On for Container Registries (Manual)

Profile Applicability:

- Level 2

Description:

Turning on Azure Defender enables threat detection for Container Registries, providing threat intelligence, anomaly detection, and behavior analytics in the Azure Security Center.

Rationale:

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

Impact:

Turning on Azure Defender in Azure Security Center incurs an additional cost per resource.

Audit:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. Review the chosen pricing tier. For the `Container Registries` resource type `Plan` should be set to `On`.

Using Azure Command Line Interface 2.0
Ensure the output of the below command is Standard

```
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/pr
icings?api-version=2018-06-01' | jq '.|.value[] |
select(.name=="ContainerRegistry")'|jq '.properties.pricingTier'
```

Using PowerShell

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

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

Remediation:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. On the line in the table for `Container Registries` Select `On` under `Plan`.
6. Select `Save`

Using Azure Command Line Interface 2.0

Use the below command to enable Standard pricing tier for Storage

```
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/pr
icings/StorageAccounts?api-version=2018-06-01 -d@"input.json"'
```

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

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/pricings/
StorageAccounts",
  "name": "ContainerRegistry",
  "type": "Microsoft.Security/pricings",
  "properties": {
    "pricingTier": "Standard"
  }
}
```

Default Value:

By default, Azure Defender off is selected.

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-endpoint-security#es-1-use-endpoint-detection-and-response-edr

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

2.8 Ensure that Azure Defender is set to On for Key Vault (Manual)

Profile Applicability:

- Level 2

Description:

Turning on Azure Defender enables threat detection for Key Vault, providing threat intelligence, anomaly detection, and behavior analytics in the Azure Security Center.

Rationale:

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

Impact:

Turning on Azure Defender in Azure Security Center incurs an additional cost per resource.

Audit:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. Review the chosen pricing tier. For the `Key Vault` resource type `Plan` should be set to `On`.

Using Azure Command Line Interface 2.0
Ensure the output of the below command is Standard

```
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/pr
icings?api-version=2018-06-01' | jq '.|.value[] |
select(.name=="KeyVaults")'|jq '.properties.pricingTier'
```

Using PowerShell

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

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

Remediation:

From Azure Console

1. Go to `Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Azure Defender plans` blade
5. On the line in the table for `Key Vault` Select `On` under `Plan`.
6. Select `Save`

Using Azure Command Line Interface 2.0

Use the below command to enable Standard pricing tier for Storage

```
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/pr
icings/StorageAccounts?api-version=2018-06-01 -d@"input.json"'
```

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

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/pricings/
StorageAccounts",
  "name": "KeyVaults",
  "type": "Microsoft.Security/pricings",
  "properties": {
    "pricingTier": "Standard"
  }
}
```

Default Value:

By default, Azure Defender off is selected.

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-identity-management#im-8-secure-user-access-to-legacy-applications

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

2.9 Ensure that Windows Defender ATP (WDATP) integration with Security Center is selected (Manual)

Profile Applicability:

- Level 2

Description:

This setting enables Windows Defender ATP (WDATP) integration with Security Center.

Rationale:

WDATP integration brings comprehensive Endpoint Detection and Response (EDR) capabilities within security center. This integration helps to spot abnormalities, detect and respond to advanced attacks on Windows server endpoints monitored by Azure Security Center. Windows Defender ATP in Security Center supports detection on Windows Server 2016, 2012 R2, and 2008 R2 SP1 operating systems in a Standard service subscription.

WDATP works only with Standard Tier subscriptions.

Impact:

WDATP works with Standard pricing tier Subscription.Choosing the Standard pricing tier of Azure Security Center incurs an additional cost per resource.

Audit:

From Azure Console

1. Go to `Azure Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Threat Detection` blade
5. Ensure setting `Allow Windows Defender ATP to access my data` is selected.

Using Azure Command Line Interface 2.0

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/$0/providers/Microsoft.Security/se
```

```
ttings?api-version=2019-01-01' | jq '.|.value[] | select(.name=="WDATP")'|jq
'.properties.enabled'
```

Remediation:

From Azure Console

1. Go to `Azure Security Center`
2. Select `Security policy` blade
3. Click On `Edit Settings` to alter the the security policy for a subscription
4. Select the `Threat Detection` blade
5. Check/Enable option `Allow Windows Defender ATP to access my data`
6. Select `Save`

Using Azure Command Line Interface 2.0

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/$0/providers/Microsoft.Security/se
ttings/WDATP?api-version=2019-01-01 -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": "DataExportSetting",
  "type": "Microsoft.Security/settings",
  "properties": {
    "enabled": true
  }
}
```

References:

1. https://docs.microsoft.com/en-in/azure/security-center/security-center-wdatp
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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-endpoint-security#es-1-use-endpoint-detection-and-response-edr
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-endpoint-security#es-2-use-centrally-managed-modern-anti-malware-software

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

2.10 Ensure that Microsoft Cloud App Security (MCAS) integration with Security Center is selected (Manual)

Profile Applicability:

- Level 2

Description:

This setting enables Microsoft Cloud App Security (MCAS) integration with Security Center.

Rationale:

Security Center 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, Security Center detects unusual or potentially harmful operations in the Azure subscription environment. Several of the preceding analytics are powered by Microsoft Cloud App Security. To benefit from these analytics, subscription must have a Cloud App Security license.

MCAS works only with Standard Tier subscriptions.

Impact:

MCAS works with Standard pricing tier Subscription.Choosing the Standard pricing tier of Azure Security Center incurs an additional cost per resource.

Audit:

From Azure Console

1. Go to `Azure Security Center`
2. Select `Pricing & settings` blade
3. Click on the subscription name
4. Select the `Threat Detection` blade
5. Ensure setting `Allow Microsoft Cloud App Security to access my data` is selected.

Using Azure Command Line Interface 2.0

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/$0/providers/Microsoft.Security/se
ttings?api-version=2019-01-01' | jq '.|.value[] | select(.name=="MCAS")'|jq
'.properties.enabled'
```

Remediation:

From Azure Console

1. Go to `Azure Security Center`
2. Select `Security policy` blade
3. Click On `Edit Settings` to alter the the security policy for a subscription
4. Select the `Threat Detection` blade
5. Check/Enable option `Allow Microsoft Cloud App Security to access my data`
6. Select `Save`

Using Azure Command Line Interface 2.0

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/$0/providers/Microsoft.Security/se
ttings/MCAS?api-version=2019-01-01 -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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-identity-management#im-8-secure-user-access-to-legacy-applications

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	10.1 Deploy and Maintain Anti-Malware Software Deploy and maintain anti-malware software on all enterprise assets.	●	●	●
v7	8 Malware Defenses Malware Defenses			

2.11 Ensure that 'Automatic provisioning of monitoring agent' is set to 'On' (Automated)

Profile Applicability:

- Level 1

Description:

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

Rationale:

When `Automatic provisioning of monitoring agent` is turned on, Azure Security Center 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:

From Azure Console

1. Go to `Security Center`
2. Click on `Pricing & Settings`
3. Click on a subscription
4. Click on `Data Collection`
5. Ensure that `Automatic provisioning` is set to `On`

Repeat the above for any additional subscriptions.

Using Azure Command Line Interface 2.0

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/$0/providers/Microsoft.Security/au
toProvisioningSettings?api-version=2017-08-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.autoProvision'
```

Using PowerShell

```
Connect-AzAccount
Get-AzSecurityAutoProvisioningSetting
```

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

Remediation:

From Azure Console

1. Go to `Security Center`
2. Click on `Pricing & Settings`
3. Click on a subscription
4. Click on `Data Collection`
5. Set `Automatic provisioning` to `On`
6. Click `save`

Repeat the above for any additional subscriptions.

Using Azure Command Line Interface 2.0

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/$0/providers/Microsoft.Security/au
toProvisioningSettings/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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-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.

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.		●	●

2.12 Ensure any of the ASC Default policy setting is not set to "Disabled" (Manual)

Profile Applicability:

- Level 1

Description:

None of the settings offered by ASC Default policy should be set to effect "Disabled".

Rationale:

A security policy defines the desired configuration of your workloads and helps ensure compliance with company or regulatory security requirements. ASC Default policy is associated with every subscription by default. ASC default policy assignment is set of security recommendations based on best practices. Enabling recommendations in ASC default policy ensures that Azure security center provides ability to monitor all of the supported recommendations and allow automated action optionally for few of the supported recommendations.

Audit:

From Azure Console

1. Go to Azure Security Center
2. Click On the `security policy` to Open Policy Management Blade.
3. Click `Subscription View`
4. Click on `Subscription Name` to open Security Policy Blade for the Subscription.
5. Expand All the available sections `Compute And Apps`, `Data`, `Identity`
6. Ensure that any of the setting is not set to `Disabled`

The 'View effective Policy' button can be used to see all effects of policies even if they have not been modified.

Using Azure Command Line Interface 2.0

Ensure the output of the below command does not contains any setting which is set to `Disabled` or Empty

```
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.Authorizati
on/policyAssignments/SecurityCenterBuiltIn?api-version=2018-05-01'
```

Note policies that have not been modified will not be listed in this output

Remediation:

From Azure Console

1. Navigate to `Azure Policy`
2. On Policy "Overview" blade, Click on Policy `ASC Default (Subscription:Subscription_ID)`
3. On "ASC Default" blade, Click on `Edit Assignments`
4. In section `PARAMETERS`, configure the impacted setting to any other available value than `Disabled` or empty
5. Click `Save`

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/resources/policyassignments/get
6. https://docs.microsoft.com/en-us/rest/api/resources/policyassignments/create
7. https://docs.microsoft.com/en-in/azure/security-center/tutorial-security-policy
8. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-incident-response#ir-2-preparation--setup-incident-notification

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.			●

2.13 Ensure 'Additional email addresses' is configured with a security contact email (Automated)

Profile Applicability:

- Level 1

Description:

Security Center 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:

Azure Security Center 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:

From Azure Console

1. Go to `Security Center`
2. Click on `Pricing & settings`
3. Click on the appropriate Management Group, Subscription, or Workspace
4. Click on `Email notifications`
5. Ensure that a valid security contact email address is listed in the `Additional email addresses` field

Using Azure Command Line Interface 2.0
Ensure the output of the below command is set 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=2017-08-01-preview' | jq '.|.value[] |
select(.name=="default")'|jq '.properties.email'
```

Remediation:

From Azure Console

1. Go to `Security Center`
2. Click on `Pricing & settings`
3. Click on the appropriate Management Group, Subscription, or Workspace
4. Click on `Email notifications`
5. Enter a valid security contact email address (or multiple addresses separated by commas) in the `Additional email addresses` field
6. Click `Save`

Using Azure Command Line Interface 2.0

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/default1?api-version=2017-08-01-preview -d@"input.json"'
```

Where `input.json` contains the Request body json data as mentioned below. And replace validEmailAddress with email ids csv for multiple.

```
    {
      "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/securitycontacts/update

4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-incident-response#ir-2-preparation--setup-incident-notification

Additional Information:

- Excluding any of the entries in recommendations block in `input.json` 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	3 Continuous Vulnerability Management Continuous Vulnerability Management			

2.14 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:

From Azure Console

1. 1.Go to `Security Center`
2. Click on `Pricing & settings`
3. Click on the appropriate Management Group, Subscription, or Workspace
4. Click on `Email notifications`
5. Ensure that the `Notify about alerts with the following severity (or higher)` setting is checked and set to `High`

Using Azure Command Line Interface 2.0
Ensure the output of below command is set to `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/$0/providers/Microsoft.Security/se
curityContacts?api-version=2017-08-01-preview' | jq '.|.value[] |
select(.name=="default1")'|jq '.properties.alertNotifications'
```

Remediation:

From Azure Console

1. Go to `Security Center

2. Click on `Pricing & settings`
3. Click on the appropriate Management Group, Subscription, or Workspace
4. Click on `Email notifications`
5. 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
6. Click `Save`

Using Azure Command Line Interface 2.0

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/se
curityContacts/default1?api-version=2017-08-01-preview -d@"input.json"'
```

Where `input.json` contains the Request body json data as mentioned below.
And replace `validEmailAddress` with email ids csv for multiple.

```
       {
      "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, `Send email notification for high severity alerts` is not set.

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/securitycontacts/update
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-incident-response#ir-2-preparation--setup-incident-notification

Additional Information:

- Excluding any of the entries in recommendations block in `input.json` disables the specific setting by default
- Microsoft has recently changed Rest APIs to get and Update Security Contact Information. This recommendation is updated accordingly

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	17.1 Designate Personnel to Manage Incident Handling Designate one key person, and at least one backup, who will manage the enterprise's incident handling process. Management personnel are responsible for the coordination and documentation of incident response and recovery efforts and can consist of employees internal to the enterprise, third-party vendors, or a hybrid approach. If using a third-party vendor, designate at least one person internal to the enterprise to oversee any third-party work. Review annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	3 Continuous Vulnerability Management Continuous Vulnerability Management			

2.15 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:

From Azure Console

1. Go to `Security Center`
2. Click on `Pricing & settings`
3. Click on the appropriate Management Group, Subscription, or Workspace
4. Click on `Email notifications`
5. Ensure that `All users with the following roles` is set to `Owner`

Using Azure Command Line Interface 2.0
Ensure the output of below command is set to `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/$0/providers/Microsoft.Security/se
curityContacts?api-version=2017-08-01-preview' | jq '.|.value[] |
select(.name=="default1")'|jq '.properties.alertsToAdmins'
```

Remediation:

From Azure Console

1. Go to `Security Center`
2. Click on `Pricing & settings`
3. Click on the appropriate Management Group, Subscription, or Workspace
4. Click on `Email notifications`

5. In the drop down of the `All users with the following roles` field select `Owner`
6. Click `Save`

Using Azure Command Line Interface 2.0

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 Request body json data as mentioned below.
And replace `validEmailAddress` with email ids csv for multiple.

```
    {
      "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, `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/securitycontacts/update
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-incident-response#ir-2-preparation--setup-incident-notification

Additional Information:

-Excluding any of the entries in recommendations block in input.json 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	3 Continuous Vulnerability Management Continuous Vulnerability Management			

3 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.

3.1 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:

From Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Configuration`
3. Ensure that `Secure transfer required` is set to `Enabled`

Using Azure Command Line Interface 2.0

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]
```

Remediation:

From Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Configuration`
3. Set `Secure transfer required` to `Enabled`

Using Azure Command Line Interface 2.0

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-4-encrypt-sensitive-information-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.		●	●

3.2 Ensure that storage account access keys are periodically regenerated (Manual)

Profile Applicability:

- Level 1

Description:

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 in these keys being compromised.

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 that use the access key to access the storage account must be updated to use the new key.

Audit:

From Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Activity log`
3. Under `Timespan` drop-down, select `Custom` and choose `Start time` and `End time` such that it ranges 90 days
4. Enter `RegenerateKey` in the `Search` text box
5. Click `Apply`

It should list out all `RegenerateKey` events. If no such event exists, then this is a finding.
Using Azure Command Line Interface 2.0

1. Get a list of storage accounts**

```
az storage account list
```

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:

Follow Microsoft Azure documentation for regenerating storage account access keys.

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-1-protect-and-limit-highly-privileged-users
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-identity-management#im-2-manage-application-identities-securely-and-automatically
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-identity-and-privileged-access-strategy

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	6.2 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	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
	revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	16 Account Monitoring and Control Account Monitoring and Control			

3.3 Ensure Storage logging is enabled for Queue service for read, write, and delete requests (Manual)

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.

Audit:

From Azure Console:

1. Go to `Storage Accounts`.
2. Select the specific Storage Account.
3. Click the `Diagnostics settings (classic)` blade from `Monitoring (classic)` section.
4. Ensure the `Status` is set to `On`, if set to `Off`.
5. Select `Queue properties`.
6. Ensure `Read` `Write` `Delete` options are selected under the `Logging` section.

Using Azure Command Line Interface 2.0:
Ensure the below command's output contains properties `delete`, `read` and `write` set to `true`.

```
az storage logging show --services q --account-name <storageAccountName>
```

Remediation:

From Azure Console:

1. Go to `Storage Accounts`.
2. Select the specific Storage Account.
3. Click the `Diagnostics settings (classic)` blade from `Monitoring (classic)` section.
4. Set the `Status` to `On`, if set to `Off`.
5. Select `Queue properties`.
6. Select `Read`, `Write` and `Delete` options under the `Logging` section to enable Storage Logging for Queue service.

Using Azure Command Line Interface 2.0

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
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

Additional Information:

By the nature and intent of having queues, practically we cannot generalize detailed audit log requirement for every queue. This recommendation may be applicable to storage account queue 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.		●	●

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.		●	●

3.4 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.
From Azure Console

1. Go to Storage Accounts
2. For each storage account, go to Shared access signature
3. Set Start and expiry date/time within an hour

note At this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

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

CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	5.3 Disable Dormant Accounts Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●
v7	16.10 Ensure All Accounts Have An Expiration Date Ensure that all accounts have an expiration date that is monitored and enforced.		●	●

3.5 Ensure that 'Public access level' is set to Private for blob containers (Automated)

Profile Applicability:

- Level 1

Description:

Disable anonymous access to blob containers and disallow blob public access on storage account.

Rationale:

Anonymous, public read access to a container and its blobs can be enabled in Azure Blob storage. 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 anonymous access to blob containers until, and unless, it is strongly desired. A shared access signature token should be used for providing controlled and timed access to blob containers. If no anonymous access is needed on the storage account, it's recommended to set allowBlobPublicAccess false.

Impact:

Access using shared access signatures will have to be managed.

Audit:

From Azure Console

1. Go to `Storage Accounts`
2. For each storage account, go to `Containers` under `BLOB SERVICE`
3. For each container, click `Access policy`
4. Ensure that `Public access level` is set to `Private (no anonymous access)`
5. For each storage account, go to Allow Blob public access` in Configuration
6. Ensure `Disabled` if no anonymous access is needed on the storage account

Using Azure Command Line Interface 2.0
Ensure the below command output contains null

```
az storage container list  --account-name <accountName> --account-key
<accountKey> --query '[*].properties.publicAccess'
```

Ensure allowBlobPublicAccess is false

```
az storage account show --name <storage-account> --resource-group <resource-group> --query allowBlobPublicAccess --output tsv
```

Remediation:

From Azure Console

First, follow Microsoft documentation and created shared access signature tokens for your blob containers. Then,

1. Go to `Storage Accounts`
2. For each storage account, go to `Containers` under `BLOB SERVICE`
3. For each container, click `Access policy`
4. Set `Public access level` to `Private (no anonymous access)`
5. For each storage account, go to `Allow Blob public access` in Configuration
6. Set `Disabled` if no anonymous access is needed on the storage account

Using Azure Command Line Interface 2.0

1. Identify the container name from the audit command
2. Set the permission for public access to `private`(off) for the above container name, using the below command

```
az storage container set-permission --name <containerName> --public-access off --account-name <accountName> --account-key <accountKey>
```

3. Set Disabled if no anonymous access is wanted on the storage account

```
az storage account update --name <storage-account> --resource-group <resource-group> --allow-blob-public-access false
```

Default Value:

By default, `Public access level` is set to `Private (no anonymous access)` for blob containers. By default, AllowBlobPublicAccess is set to Null (allow in effect) for storage account.

References:

1. https://docs.microsoft.com/en-us/azure/storage/blobs/storage-manage-access-to-resources
2. https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-1-implement-security-for-internal-traffic

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	16 Account Monitoring and Control Account Monitoring and Control			

3.6 Ensure default network access rule for Storage Accounts is set to deny (Automated)

Profile Applicability:

- Level 2

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.

Audit:

From Azure Console

1. Go to Storage Accounts
2. For each `storage account`, Click on the settings menu called `Firewalls` and `virtual networks`.
3. Ensure that Allow access from `All networks` is not selected.

Using Azure Command Line Interface 2.0

Ensure `defaultAction` is not set to `Allow`.

```
az storage account list --query '[*].networkRuleSet'
```

Remediation:

From Azure Console

1. Go to `Storage Accounts`

2. For each storage account, Click on the `settings` menu called `Firewalls` and `virtual networks`.
3. Ensure that you have elected to allow access from `Selected networks`.
4. Add rules to `allow traffic` from `specific network`.
5. Click Save to apply your changes.

Using Azure Command Line Interface 2.0

Use the below command to update `default-action` to `Deny`.

```
    az storage account update --name <StorageAccountName> --resource-group
<resourceGroupName> --default-action Deny
```

References:

1. https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-1-implement-security-for-internal-traffic

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	16 Account Monitoring and Control Account Monitoring and Control			

3.7 Ensure 'Trusted Microsoft Services' is enabled for Storage Account access (Manual)

Profile Applicability:

- Level 2

Description:

Some Microsoft services that interact with storage accounts operate from networks that can't be granted access through network rules. To help this type of service work as intended, allow the set of trusted Microsoft services to bypass the network rules. These services will then use strong authentication to access the storage account. If the Allow trusted Microsoft services exception is enabled, the following services: Azure Backup, Azure Site Recovery, Azure DevTest Labs, Azure Event Grid, Azure Event Hubs, Azure Networking, Azure Monitor and Azure SQL Data Warehouse (when registered in the subscription), are granted access to the storage account.

Rationale:

Turning on firewall rules for storage account will block access to incoming requests for data, including from other Azure services. This includes using the Portal, writing logs, etc. We can re-enable functionality. The customer can get access to services like Monitor, Networking, Hubs, and Event Grid by enabling `"Trusted Microsoft Services"` through exceptions. Also, Backup and Restore of Virtual Machines using unmanaged disks in storage accounts with network rules applied is supported via creating an exception.

Audit:

From Azure Console

1. Go to `Storage Accounts`
2. For each storage account, Click on the settings menu called `Firewalls` and `virtual networks`.
3. Click on `Selected networks`.
4. Ensure that `Allow trusted Microsoft services to access this storage account` is checked in `Exceptions`.

Using Azure Command Line Interface 2.0

Ensure `bypass` contains `AzureServices`

```
az storage account list --query '[*].networkRuleSet'
```

Remediation:

From Azure Console

1. Go to `Storage Accounts`
2. For each storage account, Click on the settings menu called `Firewalls` and `virtual networks`.
3. Ensure that you have elected to allow access from 'Selected networks'.
4. Enable check box for `Allow trusted Microsoft services to access this storage account`.
5. Click Save to apply your changes.

Using Azure Command Line Interface 2.0

Use the below command to update `trusted Microsoft services`.

```
    az storage account update --name <StorageAccountName> --resource-group
<resourceGroupName> --bypass AzureServices
```

References:

1. https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-1-implement-security-for-internal-traffic
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy

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	9.2 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.		●	●

3.8 Ensure soft delete is enabled for Azure Storage (Automated)

Profile Applicability:

- Level 1

Description:

The Azure Storage blobs contain data like ePHI, Financial, secret or personal. Erroneously modified or deleted accidentally by an application or other storage account user cause data loss or data unavailability.

It is recommended the Azure Storage be made recoverable by enabling **soft delete** configuration. This is to save and recover data when blobs or blob snapshots are deleted.

Rationale:

There could be scenarios where users accidentally run delete commands on Azure Storage blobs or blob snapshot or attacker/malicious user does it deliberately to cause disruption. Deleting an Azure Storage blob leads to immediate data loss / non-accessible data.

There is a property of Azure Storage blob service to make recoverable blobs.

- **Soft Delete**

  Enabling this configuration for azure storage ensures that even if blobs/data were deleted from the storage account, Blobs/data objects remain recoverable for a particular time which set in the "Retention policies" [Retention policies can be 7 days to 365 days].

Audit:

From Azure Console:

1. Go to Storage Account
2. For each Storage Account, navigate to Data protection
3. Ensure that soft delete is enabled

Using Azure Command-Line Interface 2.0:
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
<StorageAccountName>
```

Remediation:

From Azure Console:

1. Go to Storage Account
2. For each Storage Account, navigate to `Data Protection`
3. Select set soft delete enabled and enter a number of days you want to retain soft deleted data.

Using Azure Command-Line Interface 2.0:
Update retention days in below command

```
az storage blob service-properties delete-policy update --days-retained
<RetentionDaysValue> --account-name <StorageAccountName> --enable true
```

Default Value:

When new storage account is created, soft delete is by default **disabled**.

References:

1. https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-soft-delete

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 Data Recovery Capabilities Data Recovery Capabilities			

3.9 Ensure storage for critical data are encrypted with Customer Managed Key (Automated)

Profile Applicability:

- Level 2

Description:

Enable sensitive data encryption at rest using Customer Managed Keys 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. However, if you want to control and manage this encryption key yourself, 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.

Impact:

If the key expires by setting the 'activation date' and 'expiration date' of the key, 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:

From Azure Console:

1. Go to Storage Accounts`
2. For each storage account, go to `Encryption`
3. Ensure that Encryption type is set to Customer Managed Keys

Remediation:

From Azure Console:

1. Go to `Storage Accounts`
2. For each storage account, go to `Encryption`

3. Set Customer Managed Keys
4. Select the Encryption key and enter the appropriate setting value
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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-1-discovery,-classify-and-label-sensitive-data

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.			●

3.10 Ensure Storage logging is enabled for Blob service for read, write, and delete requests (Manual)

Profile Applicability:

- Level 2

Description:

The Storage Blob service provides scalable, cost-efficient objective 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 individual requests and to diagnose issues with a storage service. Requests are logged on a best-effort basis.

Impact:

Enabling storage account blob service logging does have a cost implication.

Audit:

From Azure Console:

- Go to `Storage Accounts`.
- Select the specific Storage Account.
- Click the `Diagnostics settings (classic)` blade from `Monitoring (classic)` section.
- Ensure the `Status` is set to `On`, if set to `Off`.
- Select `Blob properties`.
- Ensure `Read`, `Write`, and `Delete` options are selected under the `Logging section`.

Using Azure Command Line Interface:
Ensure the below command's output contains properties delete, read and write set to true.

```
az storage logging show --services b --account-name <storageAccountName>
```

Remediation:

From Azure Console:

- Go to `Storage Accounts`.
- Select the specific Storage Account.
- Click the `Diagnostics settings (classic)` blade from `Monitoring (classic)` section.
- Set the `Status` to `On`, if set to `Off`.
- Select `Blob properties`.
- Select `Read`, `Write` and `Delete` options under the `Logging`section to enable Storage Logging for Blob service.

Using Azure Command Line Interface:
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, 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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

Additional Information:

By the nature and intent of having blobs, practically we cannot generalize detailed audit log requirement for every blob. This recommendation may be applicable to storage account blob 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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
	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.		●	●

3.11 Ensure Storage logging is enabled for Table service for read, write, and delete requests (Manual)

Profile Applicability:

- Level 2

Description:

The Storage Table storage is a service that stores structure 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 individual requests and to diagnose issues with a storage service. Requests are logged on a best-effort basis.

Impact:

Enabling storage account table service logging does have a cost implication.

Audit:

From Azure Console:

- Go to `Storage Accounts`.
- Select the specific Storage Account.
- Click the `Diagnostics settings (classic)` blade from `Monitoring (classic)` section.
- Ensure the `Status` is set to `On`, if set to `Off`.
- Select `Table properties`.
- Ensure `Read`, `Write`, and `Delete` options are selected under the `Logging section`.

Using Azure Command Line Interface:
Ensure the below command's output contains properties delete, read and write set to true.

```
az storage logging show --services t --account-name <storageAccountName>
```

Remediation:

From Azure Console:

- Go to `Storage Accounts`.
- Select the specific Storage Account.
- Click the `Diagnostics settings (classic)` blade from `Monitoring (classic)` section.
- Set the `Status` to `On`, if set to `Off`.
- Select `Table properties`.
- Select `Read`, `Write` and `Delete` options under the `Logging` section to enable Storage Logging for Table service.

Using Azure Command Line Interface:
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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

Additional Information:

By the nature and intent of having tables, practically we cannot generalize detailed audit log requirement for every table. 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 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.

4.1 SQL Server - Auditing

Auditing for Azure SQL Servers and SQL Databases tracks database events and writes them to an audit log Azure storage account, Log Analytics workspace or Event Hubs. Auditing helps to maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations. Auditing enables and facilitates adherence to compliance standards, although it doesn't guarantee compliance.

Default SQL Server Auditing profile set on a SQL server in inherited to all the SQL Databases which are part of the SQL server.

4.1.1 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:

From Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing`
4. Ensure that `Auditing` is set to `On`

Using Azure PowerShell
Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerAuditing -ResourceGroupName <resource group name> -
ServerName <server name>
```

Ensure that `AuditState` is set to `Enabled`.

Remediation:

From Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing`
4. Set `Auditing` to `On`

Using Azure PowerShell
Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server, enable auditing.

```
Set-AzureRmSqlServerAuditingPolicy -ResourceGroupName <resource group name> -
ServerName <server name> -AuditType <audit type> -StorageAccountName <storage
account name>
```

Default Value:

By default, `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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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 depricated 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.		●	●

4.1.2 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:

From Azure Console

1. Go to `SQL databases`
2. For each DB instance
3. Click on `Transparent data encryption`
4. Ensure that `Data encryption` is set to `On`

Using Azure Command Line Interface 2.0
Ensure the output of the below command is `Enabled`

```
az sql db tde show --resource-group <resourceGroup> --server <dbServerName> -
-database <dbName> --query status
```

Remediation:

From Azure Console

1. Go to `SQL databases`
2. For each DB instance
3. Click on `Transparent data encryption`
4. Set `Data encryption` to `On`

Using Azure Command Line Interface 2.0
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
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-5-encrypt-sensitive-data-at-rest

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			●

Controls Version	Control	IG 1	IG 2	IG 3
	authentication mechanism not integrated into the operating system, in order to access the information.			

4.1.3 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:

From Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing`
4. Select `Storage Details`
5. Ensure `Retention (days)` setting `greater than 90 days`

Using Azure PowerShell
Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerAuditing -ResourceGroupName <resource group name> -
ServerName <server name>
```

Ensure that `RetentionInDays` is set to `more than or equal to 90`

Remediation:

From Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing`

4. Select `Storage Details`
5. Set `Retention (days)` setting `greater than 90 days`
6. Select `OK`
7. Select `Save`

Using Azure PowerShell

For each Server, set retention policy for more than or equal to 90 days

```
set-AzureRmSqlServerAuditing -ResourceGroupName <resource group name> -
ServerName <server name> -RetentionInDays <Number of Days to retain the audit
logs, should be 90days minimum>
```

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://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserverauditing?view=azurermps-5.2.0
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-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.		●	●

4.2 SQL Server - Azure Defender for SQL

Azure Defender for SQL provides a layer of security, which enables customers to detect and respond to potential threats as they occur by providing security alerts on anomalous activities. Users will receive an alert upon suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access patterns. SQL Server Threat Detection alerts provide details of suspicious activity and recommend action on how to investigate and mitigate the threat.

Azure Defender for SQL may incur additional cost per SQL server.

4.2.1 Ensure that Advanced Threat Protection (ATP) on a SQL server is set to 'Enabled' (Automated)

Profile Applicability:

- Level 2

Description:

Enable "Azure Defender for SQL" on critical SQL Servers.

Rationale:

Azure Defender for SQL is a unified package for advanced SQL security capabilities. Azure Defender is available for Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics. It 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. It provides a single go-to location for enabling and managing these capabilities.

Impact:

Azure Defender for SQL is a paid feature and will incur additional cost for each SQL server.

Audit:

From Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Azure Defender for SQL`
4. Ensure that `Azure Defender for SQL` is set to `On`

Using Azure PowerShell
Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server

```
Get-AzSqlServerThreatDetectionPolicy -ResourceGroupName <resource group name>
-ServerName <server name>
```

Ensure that `ThreatDetectionState` is set to `Enabled`.

Remediation:

From Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Azure Defender for SQL`
4. Set `Azure Defender for SQL` to `On`

Using Azure PowerShell

Enable `Advanced Data Security` for a SQL Server:

```
Set-AzSqlServerThreatDetectionPolicy -ResourceGroupName <resource group name>
-ServerName <server name> -EmailAdmins $True
```

Note:

- Enabling 'Azure Defender for SQL' from the Azure portal enables `Threat Detection`
- Using Powershell command `Set-AzSqlServerThreatDetectionPolicy` enables `Azure Defender for SQL` for a SQL server

Default Value:

By default, `Azure Defender for SQL` is set to `Off`.

References:

1. https://docs.microsoft.com/en-us/azure/azure-sql/database/azure-defender-for-sql
2. https://docs.microsoft.com/cs-cz/powershell/module/azurerm.sql/get-azurermsqlserverthreatdetectionpolicy?view=azurermps-5.2.0
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-3-monitor-for-unauthorized-transfer-of-sensitive-data

Additional Information:

- The feature 'Azure Defender for SQL' can be enabled only on SQL server and the same settings will be inherently applied to the SQL databases hosted on the SQL server.

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.		●	●

4.2.2 Ensure that Vulnerability Assessment (VA) is enabled on a SQL server by setting a Storage Account (Automated)

Profile Applicability:

- Level 2

Description:

Enable Vulnerability Assessment (VA) service scans for critical SQL servers and corresponding SQL databases.

Rationale:

Enabling Azure Defender for SQL server does not enables Vulnerability Assessment capability for individual SQL databases unless storage account is set to store the scanning data and reports.

The Vulnerability Assessment service scans databases for known security vulnerabilities and highlight deviations from best practices, such as misconfigurations, excessive permissions, and unprotected sensitive data. Results of the scan include actionable steps to resolve each issue and provide customized remediation scripts where applicable. Additionally an assessment report can be customized by setting an acceptable baseline for permission configurations, feature configurations, and database settings.

Impact:

Enabling the `Azure Defender for SQL` features will incur additional costs for each SQL server.

Audit:

From Azure Console

1. Go to `SQL servers`
2. Select a server instance
3. Click on `Security Center`
4. Ensure that `Azure Defender for SQL` is set to `Enabled`
5. Select `Configure` next to `Enabled at subscription-level`
6. In Section `Vulnerability Assessment Settings`, Ensure `Storage Accounts` is does not read `Configure required settings`.

Using Azure PowerShell

Get the list of all SQL Servers

```
Get-AZSqlServer
```

For each Server

```
Get-AzSqlServerVulnerabilityAssessmentSetting -ResourceGroupName <resource
group name> -ServerName <server name>
```

Ensure that value for parameter `StorageAccountName` is not `empty` (blank).
Sample Output:

```
ResourceGroupName                       : ResourceGroup01

ServerName                              : Server01

StorageAccountName                              : mystorage

ScanResultsContainerName                : vulnerability-assessment

RecurringScansInterval                  : None

EmailSubscriptionAdmins                         : False

NotificationEmail                               : {}
```

Remediation:

From Azure Console

1. Go to `SQL servers`
2. Select a server instance
3. Click on `Security Center`
4.
    1. Select `Configure` next to `Enabled at subscription-level`
5. In Section `Vulnerability Assessment Settings`, Click `Storage Account`
6. Choose Storage Account (Existing or `Create New`). Click `Ok`
7. Click `Save`

Using Azure PowerShell

If not already, Enable `Azure Defender for a SQL`:

```
Set-AZSqlServerThreatDetectionPolicy -ResourceGroupName <resource group name>
-ServerName <server name> -EmailAdmins $True
```

To enable ADS-VA service by setting Storage Account

```
Update-AzSqlServerVulnerabilityAssessmentSetting `
            -ResourceGroupName "<resource group name>"`
            -ServerName "<Server Name>"`
            -StorageAccountName "<Storage Name from same subscription and
same Location" `
            -ScanResultsContainerName "vulnerability-assessment" `
            -RecurringScansInterval Weekly `
            -EmailSubscriptionAdmins $true `
            -NotificationEmail @("mail1@mail.com" , "mail2@mail.com")
```

Default Value:

By default Azure Defender for SQL is not enabled for a SQL server. Enabling Azure Defender for SQL does not enable VA scanning by setting Storage Account automatically.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-vulnerability-assessment
2. https://docs.microsoft.com/en-us/rest/api/sql/servervulnerabilityassessments/listbyserver
3. https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Update-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0
4. https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Get-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-6-perform-software-vulnerability-assessments

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		●	●

Controls Version	Control	IG 1	IG 2	IG 3
	scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.			

4.2.3 Ensure that VA setting Periodic Recurring Scans is enabled on a SQL server (Automated)

Profile Applicability:

- Level 2

Description:

Enable Vulnerability Assessment (VA) Periodic recurring scans for critical SQL servers and corresponding SQL databases.

Rationale:

VA setting 'Periodic recurring scans' schedules periodic (weekly) vulnerability scanning for the SQL server and corresponding Databases. Periodic and regular vulnerability scanning provides risk visibility based on updated known vulnerability signatures and best practices.

Impact:

Enabling the `Azure Defender for SQL` feature will incur additional costs for each SQL server.

Audit:

From Azure Console

1. Go to `SQL servers`
2. Select a server instance
3. Click on `Security Center`
4. Ensure that `Azure Defender for SQL` is set to `Enabled`
5. In Section `Vulnerability Assessment Settings`, Ensure `Storage Accounts` is configured.
6. In Section `Vulnerability Assessment Settings`, Ensure `Periodic recurring scans` is set to On.

Using Azure PowerShell
Get the list of all SQL Servers

```
Get-AZSqlServer
```

For each Server

```
Get-AzSqlServerVulnerabilityAssessmentSetting -ResourceGroupName <resource
group name> -ServerName <server name>
```

Ensure that value for parameter `RecurringScansInterval` is not set to `None`.
Sample Output:

```
ResourceGroupName                       : ResourceGroup01

ServerName                              : Server01

StorageAccountName                             : mystorage

ScanResultsContainerName                : vulnerability-assessment

RecurringScansInterval                  : weekly

EmailSubscriptionAdmins                        : False

NotificationEmail                              : {}
```

Remediation:

From Azure Console

1. Go to `SQL servers`
2. For each server instance
3. Click on `Security Center`
4. In Section `Vulnerability Assessment Settings`, set `Storage Account` if not already
5. Toggle 'Periodic recurring scans' to ON.
6. Click `Save`

Using Azure PowerShell
If not already, Enable `Advanced Data Security` for a SQL Server:

```
Set-AZSqlServerThreatDetectionPolicy -ResourceGroupName <resource group name>
-ServerName <server name> -EmailAdmins $True
```

To enable ADS-VA service with 'Periodic recurring scans'

```
Update-AzSqlServerVulnerabilityAssessmentSetting `
            -ResourceGroupName "<resource group name>"`
            -ServerName "<Server Name>"`
            -StorageAccountName "<Storage Name from same subscription and
same Location" `
            -ScanResultsContainerName "vulnerability-assessment" `
            -RecurringScansInterval Weekly `
            -EmailSubscriptionAdmins $true `
            -NotificationEmail @("mail1@mail.com" , "mail2@mail.com")
```

Default Value:

Enabling `Azure Defender for SQL` enables 'Periodic recurring scans' by default but does not configure the Storage account.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-vulnerability-assessment
2. https://docs.microsoft.com/en-us/rest/api/sql/servervulnerabilityassessments/listbyserver
3. https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Update-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0
4. https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Get-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-6-perform-software-vulnerability-assessments

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.		●	●

4.2.4 Ensure that VA setting Send scan reports to is configured for a SQL server (Automated)

Profile Applicability:

- Level 2

Description:

Configure 'Send scan reports to' with email ids of concerned data owners/stakeholders for a critical SQL servers.

Rationale:

Vulnerability Assessment (VA) scan reports and alerts will be sent to email ids configured at 'Send scan reports to'. This may help in reducing time required for identifying risks and taking corrective measures.

Impact:

Enabling the `Azure Defender for SQL` features will incur additional costs for each SQL server.

Audit:

From Azure Console

1. Go to `SQL servers`
2. Select a server instance
3. Click on `Security Center`
4. Ensure that `Azure Defender for SQL` is set to `Enabled`
5. Select `Configure` next to `Enabled at subscription-level`
6. In Section `Vulnerability Assessment Settings`, Ensure `Storage Accounts` is Configured.
7. In Section `Vulnerability Assessment Settings`, Ensure `Send scan reports to` is not empty.

Using Azure PowerShell
Get the list of all SQL Servers

```
Get-AZSqlServer
```

For each Server

```
Get-AzSqlServerVulnerabilityAssessmentSetting -ResourceGroupName <resource
group name> -ServerName <server name>
```

Ensure that value for parameter `NotificationEmail` is not blank/empty {}.
Sample Output:

```
ResourceGroupName                       : ResourceGroup01

ServerName                              : Server01

StorageAccountName                             : mystorage

ScanResultsContainerName                : vulnerability-assessment

RecurringScansInterval                  : weekly

EmailSubscriptionAdmins                        : False

NotificationEmail                              : {}
```

Remediation:

From Azure Console

1. Go to `SQL servers`
2. Select a server instance
3. Click on `Security Center`
4. Ensure that `Azure Defender for SQL` is set to `Enabled`
5. Select `Configure` next to `Enabled at subscription-level`
6. In Section `Vulnerability Assessment Settings`, configure `Storage Accounts` if not already
7. Configure email ids for concerned data owners/stakeholders at 'Send scan reports to'
8. Click `Save`

Using Azure PowerShell
If not already, Enable `Advanced Data Security` for a SQL Server:

```
Set-AZSqlServerThreatDetectionPolicy -ResourceGroupName <resource group name>
-ServerName <server name> -EmailAdmins $True
```

To enable ADS-VA service and Set 'Send scan reports to'

```
Update-AzSqlServerVulnerabilityAssessmentSetting `
            -ResourceGroupName "<resource group name>"`
            -ServerName "<Server Name>"`
            -StorageAccountName "<Storage Name from same subscription and
same Location" `
            -ScanResultsContainerName "vulnerability-assessment" `
```

```
            -RecurringScansInterval Weekly `
            -EmailSubscriptionAdmins $true `
            -NotificationEmail @("mail1@mail.com" , "mail2@mail.com")
```

Default Value:

By default, 'Send reports to' is blank.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-vulnerability-assessment
2. https://docs.microsoft.com/en-us/rest/api/sql/servervulnerabilityassessments/listbyserver
3. https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Update-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0
4. https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Get-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-6-perform-software-vulnerability-assessments

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.		●	●

4.2.5 Ensure that VA setting 'Also send email notifications to admins and subscription owners' is set for a SQL server (Automated)

Profile Applicability:

- Level 2

Description:

Enable Vulnerability Assessment (VA) setting 'Also send email notifications to admins and subscription owners'.

Rationale:

VA scan reports and alerts will be sent to admins and subscription owners by enabling setting 'Also send email notifications to admins and subscription owners'. This may help in reducing time required for identifying risks and taking corrective measures.

Impact:

Enabling the `Azure Defender for SQL` features will incur additional costs for each SQL server.

Audit:

From Azure Console

1. Go to `SQL servers`
2. Select a server instance
3. Click on `Security Center`
4. Ensure that `Azure Defender for SQL` is set to `Enabled`
5. Select `Configure` next to `Enabled at subscription-level`
6. In Section `Vulnerability Assessment Settings`, Ensure `Storage Accounts` is configured.
7. In Section `Vulnerability Assessment Settings`, Ensure `Also send email notifications to admins and subscription owners` is checked/enabled.

Using Azure PowerShell
Get the list of all SQL Servers

```
Get-AZSqlServer
```

For each Server

```
Get-AzSqlServerVulnerabilityAssessmentSetting -ResourceGroupName <resource
group name> -ServerName <server name>
```

Ensure that value for parameter `EmailSubscriptionAdmin` is set to true.
Sample Output:

```
ResourceGroupName                       : ResourceGroup01

ServerName                              : Server01

StorageAccountName                             : mystorage

ScanResultsContainerName                : vulnerability-assessment

RecurringScansInterval                  : weekly

EmailSubscriptionAdmins                        : False

NotificationEmail                              : {}
```

Remediation:

From Azure Console

1. Go to `SQL servers`
2. Select a server instance
3. Click on `Security Center`
4.
    1. Select `Configure` next to `Enabled at subscription-level`
5. In Section `Vulnerability Assessment Settings`, configure `Storage Accounts` if not already
6. Check/enable 'Also send email notifications to admins and subscription owners'
7. Click `Save`

Using Azure PowerShell
If not already, Enable `Advanced Data Security` for a SQL Server:

```
Set-AZSqlServerThreatDetectionPolicy -ResourceGroupName <resource group name>
-ServerName <server name> -EmailAdmins $True
```

To enable ADS-VA service and Set 'Also send email notifications to admins and subscription owners'

```
Update-AzSqlServerVulnerabilityAssessmentSetting `
            -ResourceGroupName "<resource group name>"`
            -ServerName "<Server Name>"`
            -StorageAccountName "<Storage Name from same subscription and
same Location" `
            -ScanResultsContainerName "vulnerability-assessment" `
```

```
            -RecurringScansInterval Weekly `
            -EmailSubscriptionAdmins $true `
            -NotificationEmail @("mail1@mail.com" , "mail2@mail.com")
```

Default Value:

By default, 'Also send email notifications to admins and subscription owners' is enabled.

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-vulnerability-assessment
2. https://docs.microsoft.com/en-us/rest/api/sql/servervulnerabilityassessments/listbyserver
3. https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Update-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0
4. https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Get-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-6-perform-software-vulnerability-assessments

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.		●	●

4.3 PostgreSQL Database Server

This section groups security best practices/recommendations for Azure PostgreSQL Database Servers.

4.3.1 Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable `SSL connection` on `PostgreSQL` 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:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database for PostgreSQL server`
3. For each database, click on `Connection security`
4. In `SSL` settings
5. Ensure `Enforce SSL connection` is set to `ENABLED`.

Using Azure Command Line Interface 2.0
Ensure the output of the below command returns ENABLED.

```
    az postgres server show --resource-group myresourcegroup --name
<resourceGroupName> --query sslEnforcement
```

Remediation:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to Azure Database for `PostgreSQL server`
3. For each database, click on `Connection security`
4. In `SSL` settings.
5. Click on `ENABLED` to Enforce SSL connection

Using Azure Command Line Interface 2.0

Use the below command to `enforce ssl connection` for `PostgreSQL` Database.

```
    az postgres server update --resource-group <resourceGroupName> --name
<serverName> --ssl-enforcement Enabled
```

References:

1. https://docs.microsoft.com/en-us/azure/postgresql/concepts-ssl-connection-security
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-4-encrypt-sensitive-information-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.		●	●

4.3.2 Ensure 'Enforce SSL connection' is set to 'ENABLED' for MySQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable `SSL connection` on `MYSQL` 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:

From Azure Console

1. Login to Azure Portal using https://portal.azure- list text here.com
2. Go to `Azure Database` for `MySQL server`
3. For each database, click on `Connection security`
4. In `SSL` settings
5. Ensure `Enforce SSL connection` is set to `ENABLED`.

Using Azure Command Line Interface 2.0
Ensure the output of the below command returns ENABLED.

```
   az mysql server show --resource-group myresourcegroup --name
<resourceGroupName> --query sslEnforcement
```

Remediation:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `MySQL server`
3. For each database, click on `Connection security`
4. In `SSL` settings
5. Click on `ENABLED` for `Enforce SSL connection`

Using Azure Command Line Interface 2.0

Use the below command to set MYSQL Databases to Enforce SSL connection.

```
    az mysql server update --resource-group <resourceGroupName> --name
<serverName> --ssl-enforcement Enabled
```

References:

1. https://docs.microsoft.com/en-us/azure/mysql/concepts-ssl-connection-security
2. https://docs.microsoft.com/en-us/azure/mysql/howto-configure-ssl
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-4-encrypt-sensitive-information-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.		●	●

4.3.3 Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable `log_checkpoints` on `PostgreSQL Servers`.

Rationale:

Enabling `log_checkpoints` helps the PostgreSQL Database to `Log each checkpoint` 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:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL` server
3. For each database, click on `Server parameters`
4. Search for `log_checkpoints`.
5. Ensure that value is set to `ON`.

Using Azure Command Line Interface 2.0
Ensure value is set to `ON`

```
    az postgres server configuration show  --resource-group
<resourceGroupName> --server-name <serverName> --name log_checkpoints
```

Remediation:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL` server
3. For each database, click on `Server parameters`
4. Search for `log_checkpoints`.
5. Click `ON` and save.

Using Azure Command Line Interface 2.0

Use the below command to update `log_checkpoints` configuration.

```
    az postgres server configuration set --resource-group <resourceGroupName>
--server-name <serverName> --name log_checkpoints --value 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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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.	●	●	●

4.3.4 Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable `log_connections` on `PostgreSQL Servers`.

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:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_connections`.
5. Ensure that value is set to `ON`.

Using Azure Command Line Interface 2.0

Ensure `log_connections` value is set to `ON`

```
    az postgres server configuration show --resource-group
<resourceGroupName> --server-name <serverName> --name log_connections
```

Remediation:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_connections`.
5. Click `ON` and save.

Using Azure Command Line Interface 2.0

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
```

Default Value:

By default `log_connections` is disabled (set to `off`).

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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.	●	●	●

4.3.5 Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable `log_disconnections` on `PostgreSQL Servers`.

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.

Audit:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_disconnections`.
5. Ensure that value is set to `ON`.

Using Azure Command Line Interface 2.0

Ensure `log_connections` value is set to `ON`

```
    az postgres server configuration show --resource-group
<resourceGroupName> --server-name <serverName> --name log_disconnections
```

Remediation:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_disconnections`.
5. Click `ON` and save.

Using Azure Command Line Interface 2.0

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
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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.	●	●	●

4.3.6 Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable `connection_throttling` on `PostgreSQL Servers`.

Rationale:

Enabling `connection_throttling` helps the PostgreSQL Database to `Set the verbosity of logged messages` which 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:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `connection_throttling`.
5. Ensure that value is set to `ON`.

Using Azure Command Line Interface 2.0

Ensure `connection_throttling` value is set to `ON`

```
    az postgres server configuration show --resource-group
<resourceGroupName> --server-name <serverName> --name connection_throttling
```

Remediation:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `connection_throttling`.

5. Click ON and save.

Using Azure Command Line Interface 2.0

Use the below command to update `connection_throttling` configuration.

```
    az postgres server configuration set --resource-group <resourceGroupName>
--server-name <serverName> --name connection_throttling --value 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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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.	●	●	●

4.3.7 Ensure server parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server (Automated)

Profile Applicability:

- Level 1

Description:

Enable `log_retention_days` on `PostgreSQL Servers`.

Rationale:

Enabling `log_retention_days` helps PostgreSQL Database to `Sets number of days a log file is retained` 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.

Audit:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_retention_days`.
5. Ensure that `value greater than 3`.

Using Azure Command Line Interface 2.0

Ensure `log_retention_days` value is greater than 3.

```
    az postgres server configuration show --resource-group
<resourceGroupName> --server-name <serverName> --name log_retention_days
```

Remediation:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Server parameters`
4. Search for `log_retention_days`.
5. Enter value in range 4-7 (inclusive) and save.

Using Azure Command Line Interface 2.0

Use the below command to update `log_retention_days` configuration.

```
    az postgres server configuration set --resource-group
<resourceGroupName> --server-name <serverName> --name log_retention_days --
value <4-7>
```

References:

1. https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal
2. https://docs.microsoft.com/en-us/rest/api/postgresql/configurations/listbyserver
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-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.		●	●

4.3.8 Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled (Manual)

Profile Applicability:

- Level 1

Description:

Disable access from Azure services to PostgreSQL Database 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, setup firewall rules to allow access from specific network ranges or VNET rules to allow access from specific virtual networks.

Audit:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Connection security`
4. In `Firewall rules`
5. Ensure Allow access to Azure services is set to `OFF`.

Using Azure Command Line Interface 2.0
Ensure the output of the below command does not include a rule with the name AllowAllAzureIps or "startIpAddress": "0.0.0.0" & "endIpAddress": "0.0.0.0",

```
az postgres server firewall-rule list --resource-group <resourceGroupName>  -
-server <serverName>
```

Remediation:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Azure Database` for `PostgreSQL server`
3. For each database, click on `Connection security`
4. In `Firewall rules`
5. Ensure Allow access to Azure services is set to `OFF`.

6. Click `Save` to apply the changed rule.

Using Azure Command Line Interface 2.0

Use the below command to delete the AllowAllAzureIps rule for PostgreSQL Database.

```
az postgres server firewall-rule delete --name AllowAllAzureIps  --resource-
group <resourceGroupName> --server-name <serverName>
```

References:

1. https://docs.microsoft.com/en-us/azure/postgresql/concepts-firewall-rules
2. https://docs.microsoft.com/en-us/azure/postgresql/howto-manage-firewall-using-cli
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-1-implement-security-for-internal-traffic
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-4-protect-applications-and-services-from-external-network-attacks
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-1-implement-security-for-internal-traffic

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	13.10 Perform Application Layer Filtering Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.			●
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	9.5 Implement Application Firewalls Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized traffic should be blocked and logged.			●
v7	14.2 Enable Firewall Filtering Between VLANs Enable firewall filtering between VLANs to ensure that only authorized systems		●	●

Controls Version	Control	IG 1	IG 2	IG 3
	are able to communicate with other systems necessary to fulfill their specific responsibilities.			

4.4 Ensure that Azure Active Directory Admin is configured (Automated)

Profile Applicability:

- Level 1

Description:

Use Azure Active Directory Authentication for authentication with SQL Database.

Rationale:

Azure Active Directory authentication is a mechanism to connect to Microsoft Azure SQL Database and SQL Data Warehouse by using identities in Azure Active Directory (Azure AD). With Azure AD 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 (AAD) groups.
- It can eliminate storing passwords by enabling integrated Windows authentication and other forms of authentication supported by Azure Active Directory.
- Azure AD authentication uses contained database users to authenticate identities at the database level.
- Azure AD supports token-based authentication for applications connecting to SQL Database.
- Azure AD authentication supports ADFS (domain federation) or native user/password authentication for a local Azure Active Directory without domain synchronization.
- Azure AD 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.

Audit:

From Azure Console

1. Go to `SQL servers`
2. For each SQL server, click on `Active Directory admin`
3. Ensure that an AD account has been populated for field `Active Directory admin`

Using Azure PowerShell

Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerActiveDirectoryAdministrator -ResourceGroupName <resource
group name> -ServerName <server name>
```

Ensure Output shows `DisplayName` set to `AD account`.

Remediation:

From Azure Console

1. Go to `SQL servers`
2. For each SQL server, click on `Active Directory admin`
3. Click on `Set admin`
4. Select an admin
5. Click `Save`

Using Azure PowerShell

For each Server, set AD Admin

```
Set-AzureRmSqlServerActiveDirectoryAdministrator -ResourceGroupName <resource
group name> -ServerName <server name> -DisplayName "<Display name of AD
account to set as DB administrator>"
```

From Azure Command Line Interface 2.0

Get ObjectID of user

```
az ad user list --query "[?mail==<emailId of user>].{mail:mail,
userPrincipalName:userPrincipalName, objectId:objectId}"
```

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>
```

Default Value:

Azure Active Directory Authentication for SQL Database/Server is not enabled by default

References:

1. https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-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://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermsqlserveractivedirectoryadministrator?view=azurermps-5.2.0
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-identity-management#im-1-standardize-azure-active-directory-as-the-central-identity-and-authentication-system

Additional Information:

NOTE - Assigning an Administrator in Azure Active Directory (AAD) is just the first step. When using AAD 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 sued 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.		●	●

4.5 Ensure SQL server's TDE protector is encrypted with Customer-managed key (Automated)

Profile Applicability:

- Level 2

Description:

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 Key Vault. 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 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 also 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 E.G. Azure Keyvault).

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:

From Azure Portal:

1. Go to `SQL servers`
2. For the desired server instance
3. Click On `Transparent data encryption`
4. Ensure that `Use your own key` is set to `YES`
5. Ensure `Make selected key the default TDE protector` is checked

Using 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" GET
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

Remediation:

From Azure Console:
Go to `SQL servers`
For the desired server instance

1. Click On `Transparent data encryption`
2. Set `Use your own key` to `YES`
3. Browse through your `key vaults` to Select an existing key or create a new key in Key Vault.
4. Check `Make selected key the default TDE protector`

Using 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>]```
```

Default Value:

By Default, Microsoft managed TDE protector is enabled for a SQL server. By default option 'Use your own key' is set to 'ON'.

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/azure/security/benchmarks/security-controls-v2-identity-management#im-1-standardize-azure-active-directory-as-the-central-identity-and-authentication-system

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 ensures 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 Logging and Monitoring

This section covers security recommendations to follow to set logging and monitoring policies on an Azure Subscription.

5.1 Configuring Diagnostic Settings

The Azure Diagnostic Settings capture control/management activities performed on a subscription. 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 and/or event hub. The Diagnostic Settings, if configured properly, can ensure that all activity logs are retained for longer duration. This section has recommendations for correctly configuring the Diagnostic Settings so that all activity logs captured are retained for longer periods.

When configuring Diagnostic Settings you may choose to export in one of three ways in which you need to ensure appropriate data retention. The options are Log Analytics, Event Hub, and a Storage Account. It is important to ensure you are aware and have set retention as your organization sees fit.

5.1.1 Ensure that a 'Diagnostics Setting' exists (Automated)

Profile Applicability:

- Level 1

Description:

Enable Diagnostic settings for exporting activity logs. Diagnostic setting are available for each individual resources 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:

From Azure Console

1. Go to `Diagnostics settings`
2. Ensure that a Diagnostic status is `enabled` on all appropriate resources.

Remediation:

From Azure Console

1. Click on the resource that has a diagnostic status of `disabled`
2. Select `Add Diagnostic Settings`
3. Enter a `Diagnostic setting name`
4. Select the appropriate log, metric, and destination. (This may be Log Analytics/Storage account or Event Hub)
5. Click `save`

Repeat these step for all resources as needed.

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://docs.microsoft.com/en-us/cli/azure/monitor/log-profiles?view=azure-cli-latest#az_monitor_log_profiles_create
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-5-centralize-security-log-management-and-analysis

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.		●	●

5.1.2 Ensure Diagnostic Setting captures appropriate categories (Automated)

Profile Applicability:

- Level 1

Description:

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:

From Azure Console

1. Go to `Azure Monitor`
2. Click `Activity log`
3. Click on `Diagnostic settings`
4. Click on `Edit Settings` for the diagnostic settings entry
5. Ensure that the following categories are checked: `Administrative, Alert, Policy, and Security`

Using Azure Command Line Interface 2.0
Ensure the categories set to: `Administrative, Alert, Policy, and Security`

```
az monitor diagnostic-settings subscription list
```

AZ PowerShell cmdlets
Ensure the categories Administrative, Alert, Policy, and Security are set to Enabled:True

```
get-AzDiagnosticSetting -ResourceId subscriptions/<subscriptionID>
```

Remediation:

From Azure Console

1. Go to `Azure Monitor`

2. Click `Activity log`
3. Click on `Diagnostic settings`
4. Click on `Edit Settings` for the diagnostic settings entry
5. Ensure that the following categories are checked: `Administrative, Alert, Policy, and Security`

Using ARM Template via AZ PowerShell cmdlets

Create a file to hold the JSON

```
{
    "$schema": "https://schema.management.azure.com/schemas/2019-04-
01/deploymentTemplate.json#",
    "contentVersion": "1.0.0.0",
    "parameters": {
      "settingName": {
          "type": "String"
      },
      "workspaceId": {
          "type": "String"
      }
    },
    "resources": [
      {
        "type": "Microsoft.Insights/diagnosticSettings",
        "apiVersion": "2017-05-01-preview",
        "name": "[parameters('settingName')]",
        "dependsOn": [],
        "properties": {
          "workspaceId": "[parameters('workspaceId')]",
          "logs": [
            {
            "category": "Administrative",
            "enabled": true
            },
            {
            "category": "Alert",
            "enabled": true
            },
            {
            "category": "Autoscale",
            "enabled": false
            },
            {
            "category": "Policy",
            "enabled": true
            },
            {
            "category": "Recommendation",
            "enabled": false
            },
            {
            "category": "ResourceHealth",
            "enabled": false
            },
```

```
            {
            "category": "Security",
            "enabled": true
            },
            {
            "category": "ServiceHealth",
            "enabled": false
            }
          ]
        }
      }
    ]
}
```

Reference the JSON in the New-AzSubscriptionDeployment call

```
$OMSWorkspace = Get-AzResource  -ResourceType
"Microsoft.OperationalInsights/workspaces" -Name  <Workspace Name>
New-AzSubscriptionDeployment -Name CreateDiagnosticSetting -location eastus -
TemplateFile CreateDiagnosticSetting.jsonc -settingName "Send Activity log to
workspace" -workspaceId $OMSWorkspace.ResourceId
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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,		●	●

Controls Version	Control	IG 1	IG 2	IG 3
	date, user, timestamp, source addresses, destination addresses, and other useful elements.			

5.1.3 Ensure the storage container storing the activity logs is not publicly accessible (Automated)

Profile Applicability:

- Level 1

Description:

The storage account container containing the activity log export should not be publicly accessible.

Rationale:

Allowing public access to activity log content may aid an adversary in identifying weaknesses in the affected account's use or configuration.

Impact:

Configuring container `Access policy` to `private` will remove access from the container for everyone except owners of the storage account. Access policy needs to be set explicitly in order to allow access to other desired users.

Audit:

From Azure Console

1. Go to `Activity log`
2. Select `Export`
3. Select `Subscription`https://workbench.cisecurity.org/sections/43928/recommendations/115705/edit#
4. In section `Storage Account`, note the name of the Storage account
5. Close the `Export Audit Logs` blade. Close the `Monitor - Activity Log` blade.
6. In right column, Click service `Storage Accounts` to access Storage account blade
7. Click on the storage account name noted in step 4. This will open blade specific to that storage account
8. In Section `Blob Service` click `Containers`. It will list all the containers in next blade
9. Look for a record with container named as `insight-operational-logs`. Click . . . from right most column to open `Context menu`
10. Click `Access Policy` from `Context Menu` and ensure `Public Access Level` is set to `Private (no anonymous access)`

Using Azure Command Line Interface 2.0

1. Get storage account id configured with log profile:

```
az monitor log-profiles list --query [*].storageAccountId
```

2. Ensure the container storing activity logs (insights-operational-logs) is not publicly accessible:

```
az storage container list --account-name <Storage Account Name> --query
"[?name=='insights-operational-logs']"
```

In command output ensure `publicAccess` is set to `null`

Remediation:

From Azure Console

1. Search for `Storage Accounts` to access Storage account blade
2. Click on the storage account name
3. In Section `Blob Service` click `Containers`. It will list all the containers in next blade
4. Look for a record with container named as `insight-operational-logs`. Click . . . from right most column to open `Context menu`
5. Click `Access Policy` from `Context Menu` and set `Public Access Level` to `Private (no anonymous access)`

Using Azure Command Line Interface 2.0

```
az storage container set-permission --name insights-operational-logs --
account-name <Storage Account Name> --public-access off
```

Default Value:

By default, public access is set to null (allowing only private access) for a container with activity log export.

References:

1. https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-configure
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-1-implement-security-for-internal-traffic

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	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	6 Maintenance, Monitoring and Analysis of Audit Logs Maintenance, Monitoring and Analysis of Audit Logs			

5.1.4 Ensure the storage account containing the container with activity logs is encrypted with BYOK (Use Your Own Key) (Automated)

Profile Applicability:

- Level 2

Description:

The storage account with the activity log export container is configured to use BYOK (Use Your Own Key).

Rationale:

Configuring the storage account with the activity log export container to use BYOK (Use Your Own Key) 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.

Audit:

From Azure Console

1. Go to `Activity log`
2. Select `Export`
3. Select `Subscription`
4. In section `Storage Account`, note the name of the Storage account
5. Close the `Export Audit Logs` blade. Close the `Monitor - Activity Log` blade.
6. In right column, Click service `Storage Accounts` to access Storage account blade
7. Click on the storage account name noted in step 4. This will open blade specific to that storage account
8. In Section `SETTINGS` click `Encryption`. It will show `Storage service encryption` configuration pane.
9. Ensure `Use your own key` is checked and `Key URI` is set.

Using Azure Command Line Interface 2.0

1. Get storage account id configured with log profile:

```
az monitor log-profiles list --query [*].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`

Remediation:

From Azure Console

1. In right column, Click service `Storage Accounts` to access Storage account blade
2. Click on the storage account name
3. In Section `SETTINGS` click `Encryption`. It will show `Storage service encryption` configuration pane.
4. Check `Use your own key` which will expand `Encryption Key` Settings
5. Use option `Enter key URI` or `Select from Key Vault` to set up encryption with your own key

Using Azure Command Line Interface 2.0

```
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 Valut URI> --
encryption-key-name <KeyName> --encryption-key-version <Key Version>
```

Default Value:

By default, for a storage account `keySource` is set to `Microsoft.Storage` allowing encryption with vendor Managed key and not the BYOK (Use Your Own Key).

References:

1. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-5-encrypt-sensitive-data-at-rest

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.		●	●
v8	8.1 Establish and Maintain an Audit Log Management Process Establish and maintain an audit log management process that defines the enterprise's logging requirements. At a minimum, address the collection, review, and	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
	retention of audit logs for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	6 Maintenance, Monitoring and Analysis of Audit Logs Maintenance, Monitoring and Analysis of Audit Logs			

5.1.5 Ensure that logging for Azure KeyVault 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 Keyvault. Enabling logging for Key Vault saves information in an Azure storage account that the user provides. This creates a new container named insights-logs-auditevent automatically for the specified storage account, and this same storage account can be used for collecting logs for multiple key vaults.

Audit:

From Azure Console

1. Go to `Key vaults`
2. For each Key vault
3. Go to `Diagnostic Logs`
4. Click on `Edit Settings`
5. Ensure that `Archive to a storage account` is `Enabled`
6. Ensure that `AuditEvent` is checked and the retention days is set to `180 days or as appropriate`

Using Azure Command Line Interface 2.0
List all key vaults

```
az keyvault list
```

For each keyvault `id`

```
az monitor diagnostic-settings list --resource <id>
```

Ensure that `storageAccountId` is set as appropriate. Also, ensure that `category` and `days` are set. One of the sample outputs is as below.

```
"logs": [
        {
          "category": "AuditEvent",
          "enabled": true,
          "retentionPolicy": {
            "days": 180,
            "enabled": true
          }
        }
      ]
```

Remediation:

Follow Microsoft Azure documentation and setup Azure Key Vault Logging.

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/key-vault-logging
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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.		●	●

5.2 Monitoring using Activity Log Alerts

This section covers security recommendations to follow in order to set alerting and monitoring for critical activities on an Azure subscription.

5.2.1 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:

From Azure Console

1. Navigate to `Monitor' and then 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Security/policyAssignments/write`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Create policy assignment (policyAssignments)" has "any" level with "any" status and event is initiated by "any"`

Using Azure Command Line Interface

```
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.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.authorization/policyassignments/write"),enabled:.properti
es.enabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`
- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.authorization/policyassignments/write",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

From Azure Console

1. Go to `Monitor`
2. Select `Alerts`
3. Click On `New Alert Rule`
4. Under `Scope`, click `Select resource`
5. Select the appropriate subscription under `Filter by subscription`
6. Select `Policy Assignment` under `Filter by resource type`
7. Select `All` for `Filter by location`
8. Click on the subscription resource from the entries populated under Resource
9. Verify Selection preview shows All Policy assignment (policyAssignments) and your selected subscription name
10. Click `Done`
11. Under `Condition` click `Add Condition`
12. Select `Create policy assignment` signal
13. Click `Done`
14. Under `Action group`, select `Add action groups` and complete creation process or select appropriate action group
15. Under `Alert rule details`, enter `Alert rule name` and `Description`
16. Select appropriate resource group to save the alert to
17. Check `Enable alert rule upon creation` checkbox
18. Click `Create alert rule`

Using Azure Command Line Interface

Use the below command to create an Activity Log Alert for `Create policy assignment`

```
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/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

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

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Authorization/policyAssignments/write",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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.		●	●

5.2.2 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:

From Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Security/policyAssignments/delete`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Delete policy assignment (policyAssignments)" has "any" level with "any" status and event is initiated by "any"`

Using Azure Command Line Interface

```
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.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.authorization/policyassignments/delete"),enabled:.propert
ies.enabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`
- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.authorization/policyassignments/delete",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

From Azure Console

1. Go to `Monitor`
2. Select `Alerts`
3. Click On `New Alert Rule`
4. Under `Scope`, click `Select resource`
5. Select the appropriate subscription under `Filter by subscription`
6. Select `Policy Assignment` under `Filter by resource type`
7. Select All for Filter by location
8. Click on the subscription from the entries populated under Resource
9. Verify Selection preview shows All Policy assignment (policyAssignments) and your selected subscription name
10. Click `Done`
11. Under `Condition` click `Add Condition`
12. Select `Delete policy assignment` signal
13. Click `Done`
14. Under `Action group`, select `Add action groups` and complete creation process or select appropriate action group
15. Under `Alert rule details`, enter `Alert rule name` and `Description`
16. Select appropriate resource group to save the alert to
17. Check `Enable alert rule upon creation` checkbox
18. Click `Create alert rule`

Using Azure Command Line Interface

Use the below command to create an Activity Log Alert for `Delete policy assignment`

```
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/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

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

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Authorization/policyAssignments/delete",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

Using PowerShell AZ cmdlets

Use the below command to create an Activity Log Alert for `Delete policy assignment`

```
$ComplianceName = 'Delete Policy Assignment'
$Signal = 'Microsoft.Authorization/policyAssignments/delete'
$Category = 'Administrative'
$ResourceGroupName = 'MyResourceGroup'
$actiongroup = (Get-AzActionGroup -Name corenotifications -ResourceGroupName
$ResourceGroupName)
$ActionGroupId = (New-Object
Microsoft.Azure.Management.Monitor.Models.ActivityLogAlertActionGroup
$ActionGroup.Id)
$Subscription = (Get-AzContext).Subscription
$location = 'Global'
$scope = "/subscriptions/$($Subscription.Id)"
$alertName = "$($Subscription.Name) - $($ComplianceName)"
$conditions = @(
    New-AzActivityLogAlertCondition -Field 'category' -Equal $Category
    New-AzActivityLogAlertCondition -Field 'operationName' -Equal $Signal
)
Set-AzActivityLogAlert -Location $location -Name $alertName -
ResourceGroupName $ResourceGroupName -Scope $scope -Action $ActionGroupId -
Condition $conditions
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources
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.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
	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.		●	●

5.2.3 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:

From Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Network/networkSecurityGroups/write`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Create or Update Network Security Group (networkSecurityGroups)" has "any" level with "any" status and event is initiated by "any"`

Using Azure Command Line Interface

```
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.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.network/networksecuritygroups/write"),enabled:.properties
.enabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`

- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.network/networksecuritygroups/write",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

From Azure Console

1. Go to `Monitor`
2. Select `Alerts`
3. Click On `New Alert Rule`
4. Under `Scope`, click `Select resource`
5. Select the appropriate subscription under `Filter by subscription`
6. Select `Network Security Groups` under Filter by resource type
7. Select `All` for `Filter by location`
8. Click on the subscription resource from the entries populated under Resource
9. Verify Selection preview shows All Network Security Groups and your selected subscription name
10. Click `Done`
11. Under `Condition` click `Add Condition`
12. Select `Create or Update Network Security Group` signal
13. Click `Done`
14. Under `Action group`, select `Add action groups` and complete creation process or select appropriate action group
15. Under `Alert rule details`, enter `Alert rule name` and `Description`
16. Select appropriate resource group to save the alert to
17. Check `Enable alert rule upon creation` checkbox
18. Click `Create alert rule`

Using Azure Command Line Interface

Use the below command to create an Activity Log Alert for `Create or Update Network Security Groups`

```
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/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

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

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Network/networkSecurityGroups/write",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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.		●	●

5.2.4 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:

From Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Network/networkSecurityGroups/delete`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Delete Network Security Group (networkSecurityGroups)" has "any" level with "any" status and event is initiated by "any"`

Using Azure Command Line Interface

```
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.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.network/networksecuritygroups/delete"),enabled:.propertie
s.enabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`
- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.network/networksecuritygroups/delete",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

From Azure Console

1. Go to `Monitor`
2. Select `Alerts`
3. Click On `New Alert Rule`
4. Under `Scope`, click `Select resource`
5. Select the appropriate subscription under `Filter by subscription`
6. Select `Network Security Groups` under `Filter by resource type`
7. Select `All` for `Filter by location`
8. Click on the subscription resource from the entries populated under Resource
9. Click `Done`
10. Verify Selection preview shows Network Security Groups and your selected subscription name
11. Under `Condition` click `Add Condition`
12. Select `Delete Network Security Group` signal
13. Click `Done`
14. Under `Action group`, select `Add action groups` and complete creation process or select appropriate action group
15. Under `Alert rule details`, enter `Alert rule name` and `Description`
16. Select appropriate resource group to save the alert to
17. Check `Enable alert rule upon creation` checkbox
18. Click `Create alert rule`

Using Azure Command Line Interface

Use the below command to create an Activity Log Alert for `Delete Network Security Groups`

```
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/resourceGroups/<Resource_Group_
To
```

```
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

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

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Network/networkSecurityGroups/delete",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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.		●	●

5.2.5 Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create or Update Network Security Group Rule event.

Rationale:

Monitoring for Create or Update Network Security Group Rule events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

From Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Network/networkSecurityGroups/securityRules/write`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Create or Update Security Rule (networkSecurityGroups/securityRules)" has "any" level with "any" status and event is initiated by "any"`

Using Azure Command Line Interface

```
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.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.network/networksecuritygroups/securityrules/write"),enabl
ed:.properties.enabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`

- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.network/networksecuritygroups/securityrules/write",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

From Azure Console

1. Go to `Monitor`
2. Select `Alerts`
3. Click On `New Alert Rule`
4. Under `Scope`, click `Select resource`
5. Select the appropriate subscription under `Filter by subscription`
6. Select `Network Security Group Rules` under `Filter by resource type`
7. Select `All` for `Filter by location`
8. Click on the subscription resource from the entries populated under Resource
9. Click `Done`
10. Verify Selection preview shows Network Security Group Rules and your selected subscription name
11. Under `Condition` click `Add Condition`
12. Select `Create or Update Network Security Group Rule` signal
13. Click `Done`
14. Under `Action group`, select `Add action groups` and complete creation process or select appropriate action group
15. Under `Alert rule details`, enter `Alert rule name` and `Description`
16. Select appropriate resource group to save the alert to
17. Check `Enable alert rule upon creation` checkbox
18. Click `Create alert rule`

Using Azure Command Line Interface

Use the below command to create an Activity Log Alert for `Create or Update Network Security Groups rule`

```
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/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

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

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals":
"Microsoft.Network/networkSecurityGroups/securityRules/write",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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.		●	●

5.2.6 Ensure that activity log alert exists for the Delete Network Security Group Rule (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Delete Network Security Group Rule event.

Rationale:

Monitoring for Delete Network Security Group Rule events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

From Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Network/networkSecurityGroups/securityRules/delete`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Delete Security Rule (networkSecurityGroups/securityRules)" has "any" level with "any" status and event is initiated by "any"`

Using Azure Command Line Interface

```
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.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.network/networksecuritygroups/securityrules/delete"),enab
led:.properties.enabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`

- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.network/networksecuritygroups/securityrules/delete",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

From Azure Console

1. Go to `Monitor`
2. Select `Alerts`
3. Click On `New Alert Rule`
4. Under `Scope`, click `Select resource`
5. Select the appropriate subscription under `Filter by subscription`
6. Select `Network Security Group Rules` under `Filter by resource type`
7. Select `All` for `Filter by location`
8. Click on the subscription resource from the entries populated under Resource
9. Click `Done`
10. Verify Selection preview shows Network Security Group Rules and your selected subscription name
11. Under `Condition` click `Add Condition`
12. Select `Delete Network Security Group Rule` signal
13. Click `Done`
14. Under `Action group`, select `Add action groups` and complete creation process or select appropriate action group
15. Under `Alert rule details`, enter `Alert rule name` and `Description`
16. Select appropriate resource group to save the alert to
17. Check `Enable alert rule upon creation` checkbox
18. Click `Create alert rule`

Using Azure Command Line Interface

Use the below command to create an Activity Log Alert for `Delete Network Security Groups rule`

```
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/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

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

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals":
"Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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.		●	●

5.2.7 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:

From Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Security/securitySolutions/write`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Create or Update Security Solutions (securitySolutions)" has "any" level with "any" status and event is initiated by "any"`

Using Azure Command Line Interface

```
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.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.security/securitysolutions/write"),enabled:.properties.en
abled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`
- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.security/securitysolutions/write",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

From Azure Console

1. Go to `Monitor`
2. Select `Alerts`
3. Click On `New Alert Rule`
4. Under `Scope`, click `Select resource`
5. Select the appropriate subscription under `Filter by subscription`
6. Select `Security Solutions` under `Filter by resource type`
7. Select `All` for `Filter by location`
8. Click on the subscription resource from the entries populated under Resource
9. Click `Done`
10. Verify Selection preview shows Security Solutions and your selected subscription name
11. Under `Condition` click `Add Condition`
12. Select `Create or Update Security Solutions` signal
13. Click `Done`
14. Under `Action group`, select `Add action groups` and complete creation process or select appropriate action group
15. Under `Alert rule details`, enter `Alert rule name` and `Description`
16. Select appropriate resource group to save the alert to
17. Check `Enable alert rule upon creation` checkbox
18. Click `Create alert rule`

Using Azure Command Line Interface

Use the below command to create an Activity Log Alert for `Create or Update Security Solutions`

```
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/resourceGroups/<Resource_Group_
To
```

```
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

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

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Security",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Security/securitySolutions/write",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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.		●	●

5.2.8 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:

From Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Security/securitySolutions/delete`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Delete Security Solutions (securitySolutions)" has "any" level with "any" status and event is initiated by "any"`

Using Azure Command Line Interface

```
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.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.security/securitysolutions/delete"),enabled:.properties.e
nabled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`
- Enabled set to `True`
- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.security/securitysolutions/delete",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

From Azure Console

1. Go to `Monitor`
2. Select `Alerts`
3. Click On `New Alert Rule`
4. Under `Scope`, click `Select resource`
5. Select the appropriate subscription under `Filter by subscription`
6. Select `Security Solutions` under `Filter by resource type`
7. Select `All` for `Filter by location`
8. Click on the subscription resource from the entries populated under Resource
9. Click `Done`
10. Verify Selection preview shows Security Solutions and your selected subscription name
11. Under `Condition` click `Add Condition`
12. Select `Delete Security Solutions` signal
13. Click `Done`
14. Under `Action group`, select `Add action groups` and complete creation process or select appropriate action group
15. Under `Alert rule details`, enter `Alert rule name` and `Description`
16. Select appropriate resource group to save the alert to
17. Check `Enable alert rule upon creation` checkbox
18. Click `Create alert rule`

Using Azure Command Line Interface

Use the below command to create an Activity Log Alert for `Delete Security Solutions`

```
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/resourceGroups/<Resource_Group_
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

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

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Security",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Security/securitySolutions/delete",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

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.		●	●

5.2.9 Ensure that Activity Log Alert exists for Create or Update or Delete SQL Server Firewall Rule (Automated)

Profile Applicability:

- Level 1

Description:

Create an activity log alert for the Create or Update or Delete SQL Server Firewall Rule event.

Rationale:

Monitoring for Create or Update or Delete SQL Server Firewall Rule events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

Audit:

From Azure Console

1. Navigate to `Monitor' / 'Alerts`
2. Select `Manage alert rules`
3. Click on the Alert `Name` where Condition contains `operationName equals Microsoft.Sql/servers/firewallRules/write`
4. Hover a mouse over `Condition` to ensure it is set to `Whenever the Administrative Activity Log "Create/Update server firewall rule (servers/firewallRules)" has "any" level with "any" status and event is initiated by "any"`

Using Azure Command Line Interface

```
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.insights/ac
tivityLogAlerts?api-version=2017-04-01' | jq
'.|.value[]|{location:.location,scopes:.properties.scopes,"condition":.proper
ties.condition.allOf|.[]|select(.field=="operationName" and
.equals=="microsoft.sql/servers/firewallrules/write"),enabled:.properties.ena
bled}'
```

Ensure that an alert exists where:

- location is set to `Global`
- Scopes is set to entire subscription that is `/subscriptions/<Subscription_ID>`

- Enabled set to `True`
- Condition Matches:

```
  {
  "location": "Global",
  "scopes": [
    "/subscriptions/<Subscription_ID>"
  ],
  "condition": {
    "field": "operationName",
    "equals": "microsoft.sql/servers/firewallrules/write",
    "containsAny": null
  },
  "enabled": true
}
```

Remediation:

From Azure Console

1. Go to `Monitor`
2. Select `Alerts`
3. Click On `New Alert Rule`
4. Under `Scope`, click `Select resource`
5. Select the appropriate subscription under `Filter by subscription`
6. Select `SQL servers` under `Filter by resource type`
7. Select All for Filter by location
8. Click on the subscription from the entries populated under Resource
9. Verify Selection preview shows SQL servers and your selected subscription name
10. Under `Condition` click `Add Condition`
11. Select `All Administrative operations` signal
12. Click `Done`
13. Under `Action group`, select `Add action groups` and complete creation process or select appropriate action group
14. Under `Alert rule details`, enter `Alert rule name` and `Description`
15. Select appropriate resource group to save the alert to
16. Check `Enable alert rule upon creation` checkbox
17. Click `Create alert rule`

Using Azure Command Line Interface

Use the below command to create an Activity Log Alert for `Create or Update or Delete SQL Firewall Rule`

```
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/resourceGroups/<Resource_Group_
```

```
To
Create_Alert_In>/providers/microsoft.insights/activityLogAlerts/<Unique_Alert
_Name>?api-version=2017-04-01 -d@"input.json"'
```

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

```
{
  "location": "Global",
  "tags": {},
  "properties": {
    "scopes": [
      "/subscriptions/<Subscription_ID>"
    ],
    "enabled": true,
  "condition": {
    "allOf": [
      {
        "containsAny": null,
        "equals": "Administrative",
        "field": "category"
      },
      {
        "containsAny": null,
        "equals": "Microsoft.Sql/servers/firewallRules/write",
        "field": "operationName"
      }
    ]
  },
    "actions": {
    "actionGroups": [
      {
        "actionGroupId":
"/subscriptions/<Subscription_ID>/resourceGroups/<Resource_Group_For_Alert_Gr
oup>/providers/microsoft.insights/actionGroups/<Alert_Group>",
        "webhookProperties": null
      }
    ]
  },
  }
}
```

Configurable Parameters for command line:

```
<Resource_Group_To Create_Alert_In>
<Unique_Alert_Name>
```

Configurable Parameters for `input.json`:

```
<Subscription_ID> in scopes
<Subscription_ID> in actionGroupId
<Resource_Group_For_Alert_Group> in actionGroupId
<Alert_Group> in actionGroupId
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources

Additional Information:

Operation Name `Microsoft.Sql/servers/firewallRules/write` captures firewall rule `Delete` events as well

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.		●	●

5.3 Ensure that Diagnostic Logs are enabled for all services which support it. (Automated)

Profile Applicability:

- Level 1

Description:

Diagnostic 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, getting a secret from a Key Vault. Currently, 32 Azure resources support Diagnostic Logging (See the references 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. For example, Windows event system logs are a category of diagnostics logs for VMs, and blob, table, and queue logs are categories of diagnostics logs for storage accounts.

A number of back-end services were not configured to log and store Diagnostic Logs for certain activities or for a sufficient length. It is crucial that logging systems are correctly configured to log all relevant activities and retain those logs for a sufficient length of time. By default, Diagnostic Logs are not enabled. Given that the mean time to detection in an enterprise is 240 days, a minimum retention period of two years is recommended.

Note: The CIS Benchmark covers some specific Diagnostic Logs separately.

```
   3.3 - Ensure Storage logging is enabled for Queue service for read, write,
and delete requests



   6.4 Ensure that Network Security Group Flow Log retention period is
'greater than 90 days'
```

Rationale:

A lack of Diagnostic Logs 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, Diagnostic Logs are not enabled by default. Specifically, without Diagnostic Logs it would be impossible to tell which entities had accessed a data store that which was breached. In addition, alerts for failed attempts to access APIs for Web Services or Databases are only possible when Diagnostic Logging is enabled.

Impact:

Costs for Log Analytics Workspaces varies with Log Volume.

Audit:

From Azure Console

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

Using Azure Command Line Interface
Use the following command to list the resource manager resources.

```
az resource  list | jq '.[].id' | sed 's/\"//g' > resources.txt
```

Check if diagnostic logging was present.

```
for resource in `cat resources.txt`; do
   echo $resource &&  az monitor diagnostic-settings list --resource
$resource 2>/dev/null| jq '.value'
done
```

The output from above will give the resource id followed by `[]` if a diagnostic log is available but not present.

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 logging at first, and then be more aggressive moving data to cold storage if the volume of data

becomes a cost concern.

From Azure Console

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

Using Azure Command Line Interface

Enable logging for all resources which support Diagnostic Logs to ensure interactions within the resource are logged and available. The skeleton command for creating logs and metrics with unlimited retention on a generic resource are shown below.

```
az monitor diagnostic-settings create --resource {ID} -n {name}
                            --event-hub-rule {eventHubRuleID} --storage-
account {storageAccount}
                            --logs '[
                              {
                                "category": "WorkflowRuntime",
                                "enabled": true,
                                "retentionPolicy": {
                                  "enabled": false,
                                  "days": 0
                                }
                              }
                            ]'
                            --metrics '[
                              {
                                "category": "WorkflowRuntime",
                                "enabled": true,
                                "retentionPolicy": {
                                  "enabled": false,
                                  "days": 0
                                }
                              }
                            ]'
```

Default Value:

Disabled

References:

1. [Azure: Logs and Audit - Fundamentals](https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit)[Azure: Collecting Logs](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-activity-logs)\ [Azure KeyVault: Logging](https://docs.microsoft.com/en-us/azure/key-vault/key-vault-logging)\ [Azure: Monitor Diagnostic Settings](https://docs.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?view=azure-cli-latest)\ [Azure: Overview of Diagnostic Logs](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-logs-overview)\ [Azure: Supported Services for Diagnostic Logs](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-logs-schema)\ [Azure: Diagnostic Logs for CDNs](https://docs.microsoft.com/en-us/azure/cdn/cdn-azure-diagnostic-logs)\
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-4-enable-logging-for-azure-resources
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-5-centralize-security-log-management-and-analysis
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-5-centralize-security-log-management-and-analysis

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.		●	●
v7	7.6 Log all URL requests Log all URL requests from each of the organization's systems, whether onsite or a		●	●

Controls Version	Control	IG 1	IG 2	IG 3
	mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.			

6 Networking

This section covers security recommendations to follow in order to set networking policies on an Azure subscription.

6.1 Ensure that RDP access is restricted from the internet (Automated)

Profile Applicability:

- Level 1

Description:

Disable RDP access on network security groups from the Internet.

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:

From Azure Console

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`,
    - Source = `Any` OR `Internet`

Using Azure Command Line Interface 2.0
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"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or
"any"
```

Remediation:

Disable direct RDP access to your Azure Virtual Machines from the Internet. After direct RDP access from the Internet is disabled, you have other options you can use to access these virtual machines for remote management:

- Point-to-site VPN
- Site-to-site VPN
- ExpressRoute

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-1-implement-security-for-internal-traffic

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.	●	●	●
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.		●	●

6.2 Ensure that SSH access is restricted from the internet (Automated)

Profile Applicability:

- Level 1

Description:

Disable SSH access on network security groups from the Internet.

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:

From Azure Console

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`,
    - Source = `Any` OR `Internet`

Using Azure Command Line Interface 2.0
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"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or
"any"
```

Remediation:

Disable direct SSH access to your Azure Virtual Machines from the Internet. After direct SSH access from the Internet is disabled, you have other options you can use to access these virtual machines for remote management:

- Point-to-site VPN
- Site-to-site VPN
- ExpressRoute

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-1-implement-security-for-internal-traffic

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.	●	●	●
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.		●	●

6.3 Ensure no SQL Databases allow ingress 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:

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.

Impact:

Impact: Disabling `Allow access to Azure Services` will break all connections to SQL server and Hosted Databases unless custom IP specific rules are not added in Firewall Policy.

Audit:

From Azure Console

1. Go to `SQL servers`
2. For each SQL server
3. Click on `Firewall / Virtual Networks`
4. Ensure that `Allow access to Azure services` to set to `OFF`
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

Using Azure PowerShell
Get the list of all SQL Servers

```
Get-AzureRmSqlServer
```

For each Server

```
Get-AzureRmSqlServerFirewallRule -ResourceGroupName <resource group name> -
ServerName <server name>
```

Ensure that `StartIpAddress` is not set to `0.0.0.0` or other combinations which allows access to wider public IP ranges including Windows Azure IP ranges.

Remediation:

From Azure Console

1. Go to `SQL servers`
2. For each SQL server
3. Click on `Firewall / Virtual Networks`
4. Set `Allow access to Azure services` to `OFF'
5. Set firewall rules to limit access to only authorized connections

Using Azure PowerShell
Disable Default Firewall Rule `Allow access to Azure services`:
`Remove-AzureRmSqlServerFirewallRule -FirewallRuleName "AllowAllWindowsAzureIps" -ResourceGroupName <resource group name> -ServerName <server name>`
Remove custom Firewall rule:
`Remove-AzureRmSqlServerFirewallRule -FirewallRuleName "<firewallRuleName>" -ResourceGroupName <resource group name> -ServerName <server name>`
Set the appropriate firewall rules:

```
Set-AzureRmSqlServerFirewallRule -ResourceGroupName <resource group name> -
ServerName <server name> -FirewallRuleName "<Fw 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, setting `Allow access to Azure Services` is set to `ON` allowing access to all Windows Azure IP ranges.

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-1-implement-security-for-internal-traffic

Additional Information:

Firewall rules configured on individual SQL Database using Transact-sql overrides the rules set on SQL server. Azure does not provides 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	12 Boundary Defense Boundary Defense			

6.4 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 is 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.

Audit:

From Azure Console

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`

Using Azure Command Line Interface 2.0

```
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`.

Remediation:

From Azure Console

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`

Using Azure Command Line Interface 2.0

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-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.		●	●

6.5 Ensure that Network Watcher is 'Enabled' (Manual)

Profile Applicability:

- Level 1

Description:

Enable Network Watcher for Azure subscriptions.

Rationale:

Network diagnostic and visualization tools available with Network Watcher help users understand, diagnose, and gain insights to the network in Azure.

Audit:

From Azure Console

1. Go to `Network Watcher`
2. Ensure that the `STATUS` is set to `Enabled`

Using Azure Command Line Interface 2.0

```
az network watcher list
```

This will list all regions where `provisioningState` is `Succeeded`.
Then run

```
az account list-locations
```

This will list all regions that exist in the subscription. Compare this list to the previous one to Ensure that for all regions, `provisioningState` is set to `Succeeded`.

Remediation:

Opting-out of Network Watcher automatic enablement is a permanent change. Once you opt-out you cannot opt-in without contacting support.

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://docs.azure.cn/zh-cn/cli/network/watcher?view=azure-cli-latest#az_network_watcher_list
3. https://docs.azure.cn/zh-cn/cli/network/watcher?view=azure-cli-latest#az_network_watcher_configure
4. https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-create
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-3-enable-logging-for-azure-network-activities

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	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.	●	●	●

6.6 Ensure that UDP Services are restricted from the Internet (Automated)

Profile Applicability:

- Level 1

Description:

Disable Internet exposed UDP ports on network security groups.

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 source for disrupting services of other machines on the Azure Virtual Network or even attack networked devices outside of Azure.

Audit:

From Azure Console

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`

Using Azure Command Line Interface 2.0
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 configured UDP-based services]"
"direction" : "Inbound"
"protocol" : "UDP"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or
"any"
```

Remediation:

Disable direct UDP access to your Azure Virtual Machines from the Internet. After direct UDP access from the Internet is disabled, you have other options you can use to access UDP based services running on these virtual machines:
Point-to-site VPN
Site-to-site VPN
ExpressRoute

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-1-implement-security-for-internal-traffic

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.	●	●	●
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 Virtual Machines

This section covers security recommendations to follow in order to set virtual machine policies on an Azure subscription.

7.1 Ensure Virtual Machines are utilizing Managed Disks (Manual)

Profile Applicability:

- Level 1

Description:

Migrate BLOB based VHD's 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 VHD's to managed disks both from a security and cost management perspective.

Impact:

There is no operational impact of migrating to managed disks other than the benefits mentioned above.

NOTE When converting to managed disks VMs will be powered off and back on.

Audit:

From Azure Console

1. Using the search feature, go to `Virtual Machines`
2. Select `Edit columns`
3. Add `Uses managed disks` to the selected columns
4. Select `Apply`
5. Ensure virtual machine listed are using a managed disk

Using 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.

Remediation:

From Azure Console

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.
Using Powershell

```
Stop-AzVM -ResourceGroupName $rgName -Name $vmName -Force
ConvertTo-AzVMManagedDisk -ResourceGroupName $rgName -VMName $vmName
Start-AzVM -ResourceGroupName $rgName -Name $vmName
```

References:

1. https://docs.microsoft.com/en-us/azure/virtual-machines/windows/convert-unmanaged-to-managed-disks
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-1-define-asset-management-and-data-protection-strategy

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	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
	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 Data Protection Data Protection			

7.2 Ensure that 'OS and Data' disks are encrypted with CMK (Automated)

Profile Applicability:

- Level 2

Description:

Ensure that OS disks (boot volumes) and data disks (non-boot volumes) are encrypted with CMK.

Rationale:

Encrypting the IaaS VM's OS disk (boot volume), Data disks (non-boot volume) ensures that the entire content is fully unrecoverable without a key and thus protects the volume from unwarranted reads. CMK is superior encryption although requires additional planning.

Impact:

Using CMK/BYOK will entail additional management of keys.

NOTE: You must have your key vault setup to utilize this.

Audit:

From Azure Console

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.

Using PowerShell

```
$ResourceGroupName="yourResourceGroupName"
$DiskName="yourDiskName"

$disk=Get-AzDisk -ResourceGroupName $ResourceGroupName -DiskName $DiskName
$disk.Encryption.Type
```

Remediation:

From Azure Console
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 `X` 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

Using 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.
NOTE 2: This may differ for Linux Machines as 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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-5-encrypt-sensitive-data-at-rest
7. https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-enable-customer-managed-keys-powershell

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.			●

7.3 Ensure that 'Unattached disks' are encrypted with 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:

Encryption is available only on Standard tier VMs. This might cost you more.

Utilizing and maintaining Customer-managed keys will require additional work to created, protect, and rotate keys.

Audit:

From Azure Console

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'

From Azure Command Line Interface 2.0
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>"
  }
]
```

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 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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-5-encrypt-sensitive-data-at-rest

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.			●

7.4 Ensure that only approved extensions are installed (Manual)

Profile Applicability:

- Level 1

Description:

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.

Audit:

From Azure Console

1. Go to `Virtual machines`
2. For each virtual machine, go to `Settings`
3. Click on `Extensions`
4. Ensure that the listed extensions are approved for use.

From Azure Command Line Interface 2.0
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
```

Remediation:

From Azure Console

1. Go to `Virtual machines`
2. For each virtual machine, go to `Settings`
3. Click on `Extensions`
4. If there are unapproved extensions, uninstall them.

From Azure Command Line Interface 2.0

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>
```

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/azure/security/benchmarks/security-controls-v2-endpoint-security

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.	●	●	●

7.5 Ensure that the latest OS Patches for all Virtual Machines are applied (Manual)

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

The Azure Security Center 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.

Audit:

From Azure Console

1. Go to `Security Center - Recommendations`
2. 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.
Please note that at this point of time, there is no API/CLI mechanism available to programmatically conduct security assessment for this recommendation.

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities

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.	●	●	●

7.6 Ensure that the endpoint protection for all Virtual Machines is installed (Manual)

Profile Applicability:

- Level 1

Description:

Install endpoint protection for all virtual machines.

Rationale:

Installing endpoint protection systems (like Antimalware for Azure) provides for real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with 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:

From Azure Console

1. Go to `Security Center - Recommendations`
2. Ensure that there are no recommendations for `Endpoint Protection not installed on Azure VMs`

Using Azure Command Line Interface 2.0

```
az vm show -g MyResourceGroup -n MyVm -d
```

It should list below or any other endpoint extensions as one of the installed extensions.

```
EndpointSecurity || TrendMicroDSA* || Antimalware || EndpointProtection ||
SCWPAgent || PortalProtectExtension* || FileSecurity*
```

Alternatively, you can employ your own endpoint protection tool for your OS.

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.

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-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.	●	●	●

7.7 Ensure that VHD's are encrypted (Manual)

Profile Applicability:

- Level 2

Description:

VHD (Virtual Hard Disks) are stored in BLOB storage and are the old style disks that were attached to Virtual Machines, and the BLOB VHD was then leased to the VM. By Default storage accounts are not encrypted, and Azure Defender(Security Centre) would then recommend that the OS disks should be encrypted. Storage accounts can be encrypted as a whole using PMK or CMK and this should be turned on for storage accounts containing VHD's.

Rationale:

With the changes that have been made that recommend using managed disks that are encrypted by default, we need to also have a recommendation that "legacy" disk that may for a number of reasons need to be left as VHD's should also be encrypted to protect the data content.

Impact:

Depending on how the encryption is implemented will change the size of the impact, if provider managed keys(PMK) are utilised the impact is relatively low, but processes need to be put in place to regularly rotate the keys. If Customer managed keys(CMK) are utilised a key management process needs to be implemented to store and manage key rotation and thus the impact is medium to high depending on user maturity with key management.

Audit:

Using Azure Command Line Interface:
Disk Encryption for a VM can be checked in Azure CLI using the following command.

```
az vm encryption show --name MyVM -g MyResourceGroup
```

Remediation:

From Azure Portal

1. Navigate to the `storage account` that you wish to encrypt
2. Select the `encryption` option
3. Select the `key type` that you wish to use

If you wish to use an azure managed key (the default), you can save at this point and encryption will be applied to the account.
If you select customer managed key it will ask for the location of the key (The default is an Azure Keyvault) and the key name.
Once these are captured, save the configuration and the account will be encrypted using the provided key.

Using Azure Command Line Interface:

Create the Keyvault

```
az keyvault create --name "myKV" --resource-group "myResourceGroup" --
location eastus --enabled-for-disk-encryption
```

Encrypt the disk and store the key in keyvault

```
az vm encryption enable -g MyResourceGroup --name MyVM --disk-encryption-
keyvault myKV
```

Using Azure Powershell

This process uses a keyvault to store the keys

Create the Keyvault

```
New-AzKeyvault -name MyKV -ResourceGroupName myResourceGroup -Location EastUS
-EnabledForDiskEncryption
```

Encrypt the disk and store the key in keyvault

```
$KeyVault = Get-AzKeyVault -VaultName MyKV -ResourceGroupName MyResourceGroup

Set-AzVMDiskEncryptionExtension -ResourceGroupName MyResourceGroup -VMName
MyVM -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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-5-encrypt-sensitive-data-at-rest

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	13 Data Protection Data Protection			

8 Other Security Considerations

This section covers security recommendations to follow in order to set general security and operational controls on an Azure Subscription.

8.1 Ensure that the expiration date is set on all keys (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all keys in Azure Key Vault have an expiration time set.

Rationale:

Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. The `exp` (expiration time) attribute identifies the expiration time 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 time for all keys. This ensures that the keys cannot be used beyond their assigned lifetimes.

Impact:

Keys cannot be used beyond their assigned expiration times respectively. Keys need to be rotated periodically wherever they are used.

Audit:

From Azure Console

1. Go to `Key vaults`
2. For each Key vault, click on `Keys`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Then ensure that each key in the vault has `EXPIRATION DATE` set as appropriate

Using Azure Command Line Interface 2.0
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 <KEYVALUTNAME> --query
[*].[{"kid":kid},{"enabled":attributes.enabled},{"expires":attributes.expires
}]
```

Remediation:

From Azure Console

1. Go to `Key vaults`
2. For each Key vault, click on `Keys`.
3. Under the `Settings` section, Make sure `Enabled?` is set to Yes
4. Set an appropriate `EXPIRATION DATE` on all keys.

Using Azure Command Line Interface 2.0

Update the `EXPIRATION DATE` for the key using below command.

```
az keyvault key set-attributes --name <keyName> --vault-name <vaultName> --
expires Y-m-d'T'H:M:S'Z'
```

Note:

In order to access expiration time on all keys in Azure Key Vault using Microsoft API requires "List" Key permission.

To provide required access follow below steps,

1. Go to `Key vaults`
2. For each Key vault, click on `Access Policy`.
3. Add access policy with `Key permission` as `List`

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-1-define-asset-management-and-data-protection-strategy

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.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	13 Data Protection Data Protection			

8.2 Ensure that the expiration date is set on all Secrets (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that all Secrets in the Azure Key Vault have an expiration time 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 time) attribute identifies the expiration time 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 time for all secrets. This ensures that the secrets cannot be used beyond their assigned lifetimes.

Impact:

Secrets cannot be used beyond their assigned expiry times respectively. Secrets need to be rotated periodically wherever they are used.

Audit:

From Azure Console

1. Go to `Key vaults`
2. For each Key vault, click on `Secrets`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Ensure that each secret in the vault has `EXPIRATION DATE` set as appropriate

Using Azure Command Line Interface 2.0
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
[*].[{"id":id},{"enabled":attributes.enabled},{"expires":attributes.expires}]
```

Remediation:

From Azure Console

1. Go to `Key vaults`

2. For each Key vault, click on `Secrets`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Set an appropriate `EXPIRATION DATE` on all secrets.

Using Azure Command Line Interface 2.0

Use the below command to set `EXPIRATION DATE` on the all secrets.

```
az keyvault secret set-attributes --name <secretName> --vault-name
<vaultName> --expires Y-m-d'T'H:M:S'Z'
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-4-set-up-emergency-access-in-azure-ad
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-5-automate-entitlement-management
5. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-8-choose-approval-process-for-microsoft-support
6. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-2-define-enterprise-segmentation-strategy
7. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-identity-and-privileged-access-strategy

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	16 Account Monitoring and Control Account Monitoring and Control			

8.3 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 can't delete the resource.
- `ReadOnly` means authorized users can read a resource, but they can't delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

Audit:

From Azure Console

1. Navigate to the specific Azure Resource or Resource Group
2. Click on `Locks`
3. Ensure the lock is defined with name and description, type as `CanNotDelete` or `ReadOnly` as appropriate.

Using Azure Command Line Interface 2.0
Review the list of all locks set currently:

```
az lock list --resource-group <resourcegroupname> --resource-name
<resourcename> --namespace <Namespace> --resource-type <type> --parent ""
```

Remediation:

From Azure Console

1. Navigate to the specific Azure Resource or Resource Group
2. For each of the mission critical resource, click on `Locks`
3. Click `Add`
4. Give the lock a name and a description, then select the type, `CanNotDelete` or `ReadOnly` as appropriate

Using Azure Command Line Interface 2.0

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>
```

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

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 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			

8.4 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., as may happen in the case of accidental deletion by a user or from disruptive activity by a malicious user.

Rationale:

There could be scenarios where users accidently run delete/purge commands on key vault or attacker/malicious user does it deliberately 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 are 2 key vault properties that plays role in permanent unavailability of a key vault.

1. `enableSoftDelete`:

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 next 90days. In this span of 90 days either key vault/objects can be recovered or purged (permanent deletion). If no action is taken, after 90 days key vault and its objects will be purged.

2. `enablePurgeProtection`:

enableSoftDelete only ensures that key vault is not deleted permanently and will be recoverable for 90 days from date of deletion. However, there are chances that the key vault and/or its objects are accidentally purged and hence will not be recoverable. Setting enablePurgeProtection to "true" ensures that the key vault and its objects cannot be purged.

Enabling both the parameters on key vaults ensures that key vaults and their objects cannot be deleted/purged permanently.

Impact:

Once purge-protection and soft-delete is enabled for a key vault, the action is irreversible.

Audit:

From Azure Portal
Azure Portal does not have provision to update the respective configurations
Using Azure CLI 2.0

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 `enableSoftDelete` and `enablePurgeProtection` are set to enabled.

```
az resource show --id /subscriptions/xxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/<resourceGroupName>/providers/Microsoft.KeyVault
/vaults/<keyVaultName>
```

Remediation:

To enable "Do Not Purge" and "Soft Delete" for a Key Vault:
From Azure Portal
Azure Portal does not have provision to update the respective configurations
Using Azure CLI 2.0

```
az resource update --id /subscriptions/xxxxxx-xxxx-xxxx-xxxx-
xxxxxxxxxxxx/resourceGroups/<resourceGroupName>/providers/Microsoft.KeyVault
/vaults/<keyVaultName> --set properties.enablePurgeProtection=true
properties.enableSoftDelete=true
```

Default Value:

When a new keyvault is created, both the parameters `enableSoftDelete` and `enablePurgeProtection` are set to `null` disabling both the features.

References:

1. https://docs.microsoft.com/en-us/azure/key-vault/key-vault-soft-delete-cli
2. https://blogs.technet.microsoft.com/kv/2017/05/10/azure-key-vault-recovery-options/
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-8-define-backup-and-recovery-strategy

Additional Information:

When a key is used for SQL server TDE or Encrypting Storage Account, for corresponding key vault both the features "Do Not Purge" and "Soft Delete" are enabled by default by Azure Backend.

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 Data Recovery Capabilities Data Recovery Capabilities			

8.5 Enable role-based access control (RBAC) within Azure Kubernetes Services (Automated)

Profile Applicability:

- Level 1

Description:

Ensure that RBAC is enabled on all Azure Kubernetes Services Instances

Rationale:

Azure Kubernetes Services has the capability to integrate Azure Active Directory users and groups into Kubernetes RBAC controls within the AKS Kubernetes API Server. This should be utilized to enable granular access to Kubernetes resources within the AKS clusters supporting RBAC controls not just of the overarching AKS instance but also the individual resources managed within Kubernetes.

Impact:

If RBAC is not enabled, the granularity of permissions granted to Kubernetes resources is diminished presenting more permissions than needed to users requiring access to Kubernetes resources in AKS.

Audit:

From Azure Console

1. Go to Kubernetes Services
2. For each Kubernetes Services instance, click on Automation Script.
3. Ensure that each variable "enableRBAC" is set to true.

Using Azure Command Line Interface 2.0
Ensure that the output of the below command is not empty or null.

```
az aks show --name <AKS Instance Name> --query enableRbac --resource-group
<Resource Group Name> --subscription <Subscription ID>
```

Remediation:

WARNING: This setting cannot be changed after AKS deployment, cluster will require recreation.

Default Value:

By default, RBAC is enabled.

References:

1. https://docs.microsoft.com/en-us/azure/aks/aad-integrationhttps://kubernetes.io/docs/reference/access-authn-authz/rbac/https://docs.microsoft.com/en-us/cli/azure/aks?view=azure-cli-latest#az-aks-list
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-7-follow-just-enough-administration-least-privilege-principle

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	4 Controlled Use of Administrative Privileges Controlled Use of Administrative Privileges			
v7	14 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			

9 AppService

This section covers security recommendations for Azure AppService.

9.1 Ensure App Service Authentication is set on Azure App Service (Automated)

Profile Applicability:

- Level 2

Description:

Azure App Service Authentication is a feature that can prevent anonymous HTTP requests from reaching the API app, or authenticate those that have tokens before they reach the API 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(Azure Active Directory, Facebook, Google, Microsoft Account, and Twitter), validation, storing and refreshing of tokens, managing the authenticated sessions and injecting identity information into request headers.

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:

From Azure Console

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 / Authorization`
5. Ensure that `App Service Authentication` set to `On`

Using Command line:
To check App Service Authentication status for an existing app, run the following command,

```
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`.

Remediation:

From Azure Console

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 / Authorization`
5. Set `App Service Authentication` to `On`
6. Choose other parameters as per your requirement and Click on Save

Using Azure Command Line Interface
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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-privileged-access#pa-5-automate-entitlement-management

4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-governance-strategy#gs-6-define-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	16 Account Monitoring and Control Account Monitoring and Control			

9.2 Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service (Automated)

Profile Applicability:

- Level 1

Description:

Azure Web Apps allows sites to run under both HTTP and HTTPS by default. Web 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 request to HTTPS ports. HTTPS uses the SSL/TLS protocol to provide a secure connection, which is both encrypted and authenticated. So it is important to support HTTPS for the security benefits.

Impact:

When it is enabled, every incoming HTTP requests are redirected to the HTTPS port. It means an extra level of security will be added to the HTTP requests made to the app.

Audit:

From Azure Console

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. Ensure that `HTTPS Only` set to `On` under `Protocol Settings`

Using Azure Command Line Interface
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`.

Remediation:

From Azure Console

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. Set `HTTPS Only` to `On` under `Protocol Settings` section

Using Azure Command Line Interface

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
```

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://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-ssl#enforce-https
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-4-encrypt-sensitive-information-in-transit
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-1-implement-security-for-internal-traffic

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	7 Email and Web Browser Protections Email and Web Browser Protections			

9.3 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:

From Azure Console

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. Ensure that `Minimum TLS Version` set to `1.2` under `Protocol Settings`

Using Azure Command Line Interface
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 latest now).`

Remediation:

From Azure Console

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. Set `Minimum TLS Version` to `1.2` under `Protocol Settings` section

Using Azure Command Line Interface

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
```

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://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-4-encrypt-sensitive-information-in-transit
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-network-security#ns-1-implement-security-for-internal-traffic

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	7 Email and Web Browser Protections Email and Web Browser Protections			

9.4 Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' (Automated)

Profile Applicability:

- Level 2

Description:

Client certificates allow for the app to request a certificate for incoming requests. Only clients that have a valid certificate will be able to reach the app.

Rationale:

The TLS mutual authentication technique in enterprise environments ensures the authenticity of clients to the server. If incoming client certificates are enabled, then only an authenticated client who has valid certificates can access the app.

Impact:

Utilizing and maintaining client certificates will require additional work to obtain and managed replacement and key rotation.

Audit:

From Azure Console

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 the option `Client certificate mode` located under Incoming client certificates is set to `Require`

Using Azure Command Line Interface
To check Incoming client certificates value for an existing app, run the following command,

```
az webapp show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --
query clientCertEnabled
```

The output should return `true` if Incoming client certificates value is set to `On`.

Remediation:

From Azure Console

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 the option `Client certificate mode` located under Incoming client certificates is set to `Require`

Using Azure Command Line Interface

To set Incoming client certificates value for an existing app, run the following command:

```
az webapp update --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --
set clientCertEnabled=true
```

Default Value:

By default, incoming client certificates will be 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/security/benchmarks/security-controls-v2-data-protection#dp-4-encrypt-sensitive-information-in-transit

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 Controlled Access Based on the Need to Know Controlled Access Based on the Need to Know			

9.5 Ensure that Register with Azure Active Directory is enabled on App Service (Automated)

Profile Applicability:

- Level 1

Description:

Managed service identity in App Service makes the app more secure by eliminating secrets from the app, such as credentials in the connection strings. When registering with Azure Active Directory in the app service, the app will connect to other Azure services securely without the need of username 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:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `App Services`
3. Click on each App
4. Under the `Setting` section, Click on `Identity`
5. Ensure that `Status` set to `On`

Using Azure Command Line Interface
To check Register with Azure Active Directory 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 Azure Active Directory is not set.

Remediation:

From Azure Console

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. Set `Status` to `On`

Using Azure Command Line Interface

To set Register with Azure Active Directory feature for an existing app, run the following command:

```
az webapp identity assign --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME>
```

References:

1. https://docs.microsoft.com/en-gb/azure/app-service/app-service-web-tutorial-connect-msi
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-identity-management#im-1-standardize-azure-active-directory-as-the-central-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 'PHP version' is the latest, if used to run the web app (Manual)

Profile Applicability:

- Level 1

Description:

Periodically newer versions are released for PHP software either due to security flaws or to include additional functionality. Using the latest PHP version for web apps is recommended in order to take advantage of security fixes, if any, and/or additional functionalities of the newer version.

Rationale:

Newer versions may contain security enhancements and additional functionality. Using the latest software 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 and also verify the compatibility and support provided for any additional software against the update revision that is selected.

Audit:

From Azure Console

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 `PHP version` set to latest version available under `General settings`

NOTE: No action is required If `PHP version` is set to `Off` as PHP is not used by your web app.

Using Azure Command Line Interface

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 phpVersion
```

The output should return the latest available version of PHP.

NOTE: No action is required, If the output is empty as PHP is not used by your web app.

Remediation:

From Azure Console

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 `PHP version` to latest version available under `General settings`

NOTE: No action is required If `PHP version` is set to `Off` as PHP is not used by your web app.

Using Azure Command Line Interface

To see the list of supported runtimes:

```
az webapp list-runtimes | grep php
```

To set latest PHP version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
--php-version <VERSION>
```

Default Value:

By default, PHP 5.6 version will be used when creating a new app using the command-line tool or the Azure Portal console.

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources

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	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
	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.	●	●	●

9.7 Ensure that 'Python version' is the latest, if used to run the web app (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, newer versions are released for Python software either due to security flaws or to include additional functionality. Using the latest Python version for web apps is recommended in order to take advantage of security fixes, if any, and/or additional functionalities of the newer version.

Rationale:

Newer versions may contain security enhancements and additional functionality. Using the latest software 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 and also verify the compatibility and support provided for any additional software against the update revision that is selected.

Audit:

Using Console:

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 `Application settings`
5. Ensure that `Python version` set to the latest version available under `General settings`

NOTE: No action is required, If `Python version` is set to `Off` as Python is not used by your web app.
Using Command line:
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 pythonVersion
```

The output should return the latest available version of Python.
NOTE: No action is required, If the output is empty as Python is not used by your web app.

Remediation:

Using Console:

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 `Application settings`
5. Set `Python version` to latest version available under `General settings`

NOTE: No action is required, If `Python version` is set to `Off` as Python is not used by your web app.
Using Command Line:
To see the list of supported runtimes:

```
az webapp list-runtimes | grep python
```

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>
--python-version <VERSION>
```

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources

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.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
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 'Java version' is the latest, if used to run the web app (Manual)

Profile Applicability:

- Level 1

Description:

Periodically, newer versions are released for Java software either due to security flaws or to include additional functionality. Using the latest Java version for web apps is recommended in order 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 software 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 and also verify the compatibility and support provided for any additional software against the update revision that is selected.

Audit:

From Azure Console

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 `Application settings`
5. Ensure that `Java version` set to the latest version available under `General settings`

NOTE: No action is required If `Java version` is set to `Off` as Java is not used by your web app.

Using Azure Command Line Interface

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 javaVersion
```

The output should return the latest available version of Java.

NOTE: No action is required If no output for above command as Java is not used by your web app.

Remediation:

From Azure Console

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 `Application settings`
5. Under `General settings`, Set `Java version` to latest version available
6. Set `Java minor version` to latest version available
7. Set `Java web container` to the latest version of web container available

NOTE: No action is required If `Java version` is set to `Off` as Java is not used by your web app.

Using Azure Command Line Interface

To see the list of supported runtimes:

```
az webapp list-runtimes | grep java
```

To set latest Java version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
--java-version '1.8' --java-container 'Tomcat' --java-container-version
'<VERSION>'
```

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources

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	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
	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 'HTTP Version' is the latest, if used to run the web app (Manual)

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 web 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 and 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.

Audit:

From Azure Console

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.

Using Azure Command Line Interface

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`.

Remediation:

From Azure Console

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.

Using Azure Command Line Interface

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
```

References:

1. https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources

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	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
	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 FTP deployments are disabled (Automated)

Profile Applicability:

- Level 1

Description:

By default, Azure Functions, Web and API 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 Service Apps and Functions.

Rationale:

Azure FTP deployment endpoints are public. An attacker listening to traffic on a wifi network used by a remote employee or a corporate network could see login traffic in clear-text which would then grant them full control of the code base of the app or service. This finding is more severe if User Credentials for deployment are set at the subscription level rather than using the default Application Credentials which are unique per App.

Impact:

Any deployment workflows that rely on FTP or FTPs rather than the WebDeploy or HTTPs endpoints may be affected.

Audit:

From Azure Console 2.0 For Web Apps

1. Go to the Azure Portal
2. Select `App Services`
3. Click on an App
4. Select `Settings` > `Configuration`
5. Select `General Settings`
6. Under Platform Settings, FTP state should not be `All allowed`

From Azure Console 2.0 For Function Apps

1. Go to the Azure Portal
2. Select `App Services`
3. Click on an App Function
4. Select `Platform Features`
5. Select `Configuration`
6. Select `General Settings`

7. Under Platform Settings, FTP state should not be `All allowed`

Using Azure CLI 2.0
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": "ftp://waws-prod-dm1-
129.ftp.azurewebsites.windows.net/site/wwwroot",
    "userName": "engineer-webapp-test\\$engineer-webapp-test",
    "userPWD": "dHwjxxxxxxxxxxxxxxxxxxxxxxxxxisdk6xMgeswoqg",
}
```

The correct username to user for FTP would be `engineer-webapp-test` in the output above.

Remediation:

From Azure Console

1. Go to the Azure Portal
2. Select App Services
3. Click on an App
4. Select Settings > Configuration
5. Under Platform Settings, FTP state should be `Disabled` or `FTPS Only`

Default Value:

Enabled

References:

1. [Azure Web Service Deploy via FTP](https://docs.microsoft.com/en-us/azure/app-service/deploy-ftp)
2. [Azure Web Service Deployment](https://docs.microsoft.com/en-us/azure/app-service/overview-security)
3. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-data-protection#dp-4-encrypt-sensitive-information-in-transit
4. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities

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.		●	●

9.11 Ensure Azure Keyvaults are used to store secrets (Manual)

Profile Applicability:

- Level 2

Description:

Encryption keys ,Certificate thumbprints and Managed Identity Credentials can be coded into the APP service, this renders them visible as part of the configuration, to maintain security of these keys it is better to store in an Azure Keyvault and reference them from the Keyvault.

Rationale:

App secrets control access to the application and thus need to be secured externally to the app configuration, storing the secrets externally and referencing them in the configuration also enables key rotation without having to redeploy the app service.

Impact:

Impact is primarily during the initial setup of the application or redeploying an old app to include this functionality. This will require configuration effort to setup the keyvault and then to configure the app service to use the keyvault.

Audit:

From Azure Console

1. Login to Azure Portal using https://portal.azure.com
2. Go to `Key Vaults`
3. Ensure that key vault exists and keys are listed

Remediation:

Remediation has 2 steps

1. Setup the keyvault
2. setup the app service to use the keyvault

Set up the keyvault
Using Azure CLI
`az keyvault create --name "myKV" --resource-group "myResourceGroup" --location myLocation

Using Azure Powershell

`New-AzKeyvault -name MyKV -ResourceGroupName myResourceGroup -Location myLocation

Set up the App Service to use the keyvault

Sample JSON Template for App Service Configuration

```
{
    //...
    "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]"
                    }
                }
            ]
        }
    ]
}
```

References:

1. https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references
2. https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-identity-management#im-2-manage-application-identities-securely-and-automatically

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 Data Protection Data Protection			

Appendix: Recommendation Summary Table

Control		Set Correctly	
		Yes	No
1	**Identity and Access Management**		
1.1	Ensure that multi-factor authentication is enabled for all privileged users (Manual)	☐	☐
1.2	Ensure that multi-factor authentication is enabled for all non-privileged users (Manual)	☐	☐
1.3	Ensure guest users are reviewed on a monthly basis (Automated)	☐	☐
1.4	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled' (Manual)	☐	☐
1.5	Ensure that 'Number of methods required to reset' is set to '2' (Manual)	☐	☐
1.6	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to "0" (Manual)	☐	☐
1.7	Ensure that 'Notify users on password resets?' is set to 'Yes' (Manual)	☐	☐
1.8	Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes' (Manual)	☐	☐
1.9	Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No' (Manual)	☐	☐
1.10	Ensure that 'Users can add gallery apps to their Access Panel' is set to 'No' (Manual)	☐	☐
1.11	Ensure that 'Users can register applications' is set to 'No' (Manual)	☐	☐
1.12	Ensure that 'Guest user permissions are limited' is set to 'Yes' (Manual)	☐	☐
1.13	Ensure that 'Members can invite' is set to 'No' (Manual)	☐	☐
1.14	Ensure that 'Guests can invite' is set to 'No' (Manual)	☐	☐
1.15	Ensure that 'Restrict access to Azure AD administration portal' is set to 'Yes' (Manual)	☐	☐
1.16	Ensure that 'Restrict user ability to access groups features in the Access Pane' is set to 'No' (Manual)	☐	☐
1.17	Ensure that 'Users can create security groups in Azure Portals' is set to 'No' (Manual)	☐	☐

1.18	Ensure that 'Owners can manage group membership requests in the Access Panel' is set to 'No' (Manual)	☐	☐
1.19	Ensure that 'Users can create Microsoft 365 groups in Azure Portals' is set to 'No' (Manual)	☐	☐
1.20	Ensure that 'Require Multi-Factor Auth to join devices' is set to 'Yes' (Manual)	☐	☐
1.21	Ensure that no custom subscription owner roles are created (Automated)	☐	☐
1.22	Ensure Security Defaults is enabled on Azure Active Directory (Automated)	☐	☐
1.23	Ensure Custom Role is assigned for Administering Resource Locks (Manual)	☐	☐
2	**Security Center**		
2.1	Ensure that Azure Defender is set to On for Servers (Manual)	☐	☐
2.2	Ensure that Azure Defender is set to On for App Service (Manual)	☐	☐
2.3	Ensure that Azure Defender is set to On for Azure SQL database servers (Manual)	☐	☐
2.4	Ensure that Azure Defender is set to On for SQL servers on machines (Manual)	☐	☐
2.5	Ensure that Azure Defender is set to On for Storage (Manual)	☐	☐
2.6	Ensure that Azure Defender is set to On for Kubernetes (Manual)	☐	☐
2.7	Ensure that Azure Defender is set to On for Container Registries (Manual)	☐	☐
2.8	Ensure that Azure Defender is set to On for Key Vault (Manual)	☐	☐
2.9	Ensure that Windows Defender ATP (WDATP) integration with Security Center is selected (Manual)	☐	☐
2.10	Ensure that Microsoft Cloud App Security (MCAS) integration with Security Center is selected (Manual)	☐	☐
2.11	Ensure that 'Automatic provisioning of monitoring agent' is set to 'On' (Automated)	☐	☐
2.12	Ensure any of the ASC Default policy setting is not set to "Disabled" (Manual)	☐	☐
2.13	Ensure 'Additional email addresses' is configured with a security contact email (Automated)	☐	☐
2.14	Ensure that 'Notify about alerts with the following severity' is set to 'High' (Automated)	☐	☐
2.15	Ensure that 'All users with the following roles' is set to 'Owner' (Automated)	☐	☐
3	**Storage Accounts**		

3.1	Ensure that 'Secure transfer required' is set to 'Enabled' (Automated)	☐	☐
3.2	Ensure that storage account access keys are periodically regenerated (Manual)	☐	☐
3.3	Ensure Storage logging is enabled for Queue service for read, write, and delete requests (Manual)	☐	☐
3.4	Ensure that shared access signature tokens expire within an hour (Manual)	☐	☐
3.5	Ensure that 'Public access level' is set to Private for blob containers (Automated)	☐	☐
3.6	Ensure default network access rule for Storage Accounts is set to deny (Automated)	☐	☐
3.7	Ensure 'Trusted Microsoft Services' is enabled for Storage Account access (Manual)	☐	☐
3.8	Ensure soft delete is enabled for Azure Storage (Automated)	☐	☐
3.9	Ensure storage for critical data are encrypted with Customer Managed Key (Automated)	☐	☐
3.10	Ensure Storage logging is enabled for Blob service for read, write, and delete requests (Manual)	☐	☐
3.11	Ensure Storage logging is enabled for Table service for read, write, and delete requests (Manual)	☐	☐
4	**Database Services**		
4.1	**SQL Server - Auditing**		
4.1.1	Ensure that 'Auditing' is set to 'On' (Automated)	☐	☐
4.1.2	Ensure that 'Data encryption' is set to 'On' on a SQL Database (Automated)	☐	☐
4.1.3	Ensure that 'Auditing' Retention is 'greater than 90 days' (Automated)	☐	☐
4.2	**SQL Server - Azure Defender for SQL**		
4.2.1	Ensure that Advanced Threat Protection (ATP) on a SQL server is set to 'Enabled' (Automated)	☐	☐
4.2.2	Ensure that Vulnerability Assessment (VA) is enabled on a SQL server by setting a Storage Account (Automated)	☐	☐
4.2.3	Ensure that VA setting Periodic Recurring Scans is enabled on a SQL server (Automated)	☐	☐
4.2.4	Ensure that VA setting Send scan reports to is configured for a SQL server (Automated)	☐	☐
4.2.5	Ensure that VA setting 'Also send email notifications to admins and subscription owners' is set for a SQL server (Automated)	☐	☐
4.3	**PostgreSQL Database Server**		
4.3.1	Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server (Automated)	☐	☐

4.3.2	Ensure 'Enforce SSL connection' is set to 'ENABLED' for MySQL Database Server (Automated)	☐	☐
4.3.3	Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server (Automated)	☐	☐
4.3.4	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server (Automated)	☐	☐
4.3.5	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server (Automated)	☐	☐
4.3.6	Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server (Automated)	☐	☐
4.3.7	Ensure server parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server (Automated)	☐	☐
4.3.8	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled (Manual)	☐	☐
4.4	Ensure that Azure Active Directory Admin is configured (Automated)	☐	☐
4.5	Ensure SQL server's TDE protector is encrypted with Customer-managed key (Automated)	☐	☐
5	**Logging and Monitoring**		
5.1	**Configuring Diagnostic Settings**		
5.1.1	Ensure that a 'Diagnostics Setting' exists (Automated)	☐	☐
5.1.2	Ensure Diagnostic Setting captures appropriate categories (Automated)	☐	☐
5.1.3	Ensure the storage container storing the activity logs is not publicly accessible (Automated)	☐	☐
5.1.4	Ensure the storage account containing the container with activity logs is encrypted with BYOK (Use Your Own Key) (Automated)	☐	☐
5.1.5	Ensure that logging for Azure KeyVault is 'Enabled' (Automated)	☐	☐
5.2	**Monitoring using Activity Log Alerts**		
5.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment (Automated)	☐	☐
5.2.2	Ensure that Activity Log Alert exists for Delete Policy Assignment (Automated)	☐	☐
5.2.3	Ensure that Activity Log Alert exists for Create or Update Network Security Group (Automated)	☐	☐
5.2.4	Ensure that Activity Log Alert exists for Delete Network Security Group (Automated)	☐	☐
5.2.5	Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule (Automated)	☐	☐
5.2.6	Ensure that activity log alert exists for the Delete Network Security Group Rule (Automated)	☐	☐

5.2.7	Ensure that Activity Log Alert exists for Create or Update Security Solution (Automated)	☐	☐
5.2.8	Ensure that Activity Log Alert exists for Delete Security Solution (Automated)	☐	☐
5.2.9	Ensure that Activity Log Alert exists for Create or Update or Delete SQL Server Firewall Rule (Automated)	☐	☐
5.3	Ensure that Diagnostic Logs are enabled for all services which support it. (Automated)	☐	☐
6	**Networking**		
6.1	Ensure that RDP access is restricted from the internet (Automated)	☐	☐
6.2	Ensure that SSH access is restricted from the internet (Automated)	☐	☐
6.3	Ensure no SQL Databases allow ingress 0.0.0.0/0 (ANY IP) (Automated)	☐	☐
6.4	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' (Automated)	☐	☐
6.5	Ensure that Network Watcher is 'Enabled' (Manual)	☐	☐
6.6	Ensure that UDP Services are restricted from the Internet (Automated)	☐	☐
7	**Virtual Machines**		
7.1	Ensure Virtual Machines are utilizing Managed Disks (Manual)	☐	☐
7.2	Ensure that 'OS and Data' disks are encrypted with CMK (Automated)	☐	☐
7.3	Ensure that 'Unattached disks' are encrypted with CMK (Automated)	☐	☐
7.4	Ensure that only approved extensions are installed (Manual)	☐	☐
7.5	Ensure that the latest OS Patches for all Virtual Machines are applied (Manual)	☐	☐
7.6	Ensure that the endpoint protection for all Virtual Machines is installed (Manual)	☐	☐
7.7	Ensure that VHD's are encrypted (Manual)	☐	☐
8	**Other Security Considerations**		
8.1	Ensure that the expiration date is set on all keys (Automated)	☐	☐
8.2	Ensure that the expiration date is set on all Secrets (Automated)	☐	☐
8.3	Ensure that Resource Locks are set for mission critical Azure resources (Manual)	☐	☐
8.4	Ensure the key vault is recoverable (Automated)	☐	☐
8.5	Enable role-based access control (RBAC) within Azure Kubernetes Services (Automated)	☐	☐

9	**AppService**		
9.1	Ensure App Service Authentication is set on Azure App Service (Automated)	☐	☐
9.2	Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service (Automated)	☐	☐
9.3	Ensure web app is using the latest version of TLS encryption (Automated)	☐	☐
9.4	Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' (Automated)	☐	☐
9.5	Ensure that Register with Azure Active Directory is enabled on App Service (Automated)	☐	☐
9.6	Ensure that 'PHP version' is the latest, if used to run the web app (Manual)	☐	☐
9.7	Ensure that 'Python version' is the latest, if used to run the web app (Manual)	☐	☐
9.8	Ensure that 'Java version' is the latest, if used to run the web app (Manual)	☐	☐
9.9	Ensure that 'HTTP Version' is the latest, if used to run the web app (Manual)	☐	☐
9.10	Ensure FTP deployments are disabled (Automated)	☐	☐
9.11	Ensure Azure Keyvaults are used to store secrets (Manual)	☐	☐

Appendix: Change History

Date	Version	Changes for this version
Jul 6, 2021	1.3.1	UPDATE – XLS Export – Mapped recommendations to MITRE ATT&CK
Jul 6, 2021	1.3.1	UPDATE – Multiple – Mapped recommendations to CIS Critical Controls version 8
Oct 27, 2020	1.3.0	Update - Ensure App Service Authentication is set on Azure App Service - additional permissions required to automate this policy/rule (Ticket 8229)
Nov 12, 2020	1.3.0	DELETE - Ensure that '.Net Framework' version is the latest, if used as a part of the web app - Console location not up to date (Ticket 11599)
Nov 12, 2020	1.3.0	UPDATE - Ensure that multi-factor authentication is enabled for all privileged users - some instances of userPrincipalName misspelled as userPrincipleName (Ticket 11687)
Dec 11, 2020	1.3.0	UPDATE - Ensure storage for critical data are encrypted with Customer Managed Key - update wording in Rational and impact (Ticket 11903)
Dec 11, 2020	1.3.0	UPDATE - Ensure that 'Public access level' is set to Private for blob containers - add steps for storage account settings (Ticket 11902)
Dec 11, 2020	1.3.0	ADD - Ensure Azure Keyvaults are used to store secrets (Ticket 8982)
Dec 11, 2020	1.3.0	UPDATE - Ensure Diagnostic Setting captures appropriate categories - does not work with the new Diagnostic Setting (Ticket 11627)
Dec 11, 2020	1.3.0	ADD - Ensure VHDs are encrypted (Ticket 11609)
Jan 12, 2021	1.3.0	ADD - Ensure that Activity Log Alert exists for Delete Policy Assignment (Ticket 7707)

Jan 12, 2021	1.3.0	UPDATE - Ensure Security Defaults is enabled on Azure Active Directory - setting conflicts with the CIS Office (Microsoft) 365 Benchmark (Ticket 11935)
Jan 13, 2021	1.3.0	UPDATE - Ensure guest users are reviewed on a monthly basis - Create Dynamic Group for Guest Users and add Access Review (Ticket 11728)
Jan 15, 2021	1.3.0	ADD - 2 Recommendations in Security Center Section - 2 currently available Azure Defender bundles are missing (Ticket 11638)
Jan 15, 2021	1.3.0	UPDATE - Ensure that 'OS and Data' disks are encrypted with CMK - Powershell for changing disk encryption (Ticket 11596)
Jan 15, 2021	1.3.0	UPDATE - Ensure that Azure Active Directory Admin is configured - Concern that this is an overly simplistic recommendation (Ticket 8852)
Jan 15, 2021	1.3.0	UPATE - Ensure App Service Authentication is set on Azure App Service - App Service authentication should be level 2 not level 1 (Ticket 12063)
Jan 15, 2021	1.3.0	UPDATE - Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' - Change from level 1 to level 2 (Ticket 12064)
Jan 18, 2021	1.3.0	UPDATE - Multiple recommendations - Updated reference URLs mapping recommendations to the Azure Security Benchmark
Jan 28, 2021	1.3.0	DELETE - Ensure server parameter 'log_duration' is set to 'ON' for PostgreSQL Database Server - No clear security value (Ticket 12090)
Jan 28, 2021	1.3.0	UPDATE - Ensure that a 'Diagnostics Setting' exists - Intent of recommendation is unclear (Ticket 12092)
Jan 28, 2021	1.3.0	UPDATE - Ensure that Activity Log Alert exists for Delete Policy Assignment - Minor inconsistencies in remediation procedure (Ticket 12089)

Jan 28, 2021	1.3.0	UPDATE - Ensure that Activity Log Alert exists for Create Policy Assignment - Minor inconsistencies in remediation procedure (Ticket 12088)
Jan 28, 2021	1.3.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Network Security Group - Remediation procedure is incorrect (Ticket 12081)
Jan 28, 2021	1.3.0	UPDATE - Ensure that Activity Log Alert exists for Delete Network Security Group - Remediation procedure is incorrect (Ticket 12082)
Jan 28, 2021	1.3.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Network Security Group Rule - Remediation procedure is incorrect (Ticket 12083)
Jan 28, 2021	1.3.0	UPDATE - Ensure that activity log alert exists for the Delete Network Security Group Rule - Remediation procedure is incorrect (Ticket 12084)
Jan 28, 2021	1.3.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Security Solution - Remediation procedure is incorrect (Ticket 12085)
Jan 28, 2021	1.3.0	UPDATE - Ensure that Activity Log Alert exists for Delete Security Solution - Remediation procedure is incorrect (Ticket 12086)
Jan 28, 2021	1.3.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update or Delete SQL Server Firewall Rule - Remediation procedure is incorrect (Ticket 12087)
Jan 28, 2021	1.3.0	UPDATE - Ensure that Advanced Data Security (ADS) and Advanced Threat Protection (ATP) on a SQL server is set to 'On' - ADS and ATP changed to Azure Defender for SQL (Ticket 12124)
Jan 28, 2021	1.3.0	UPDATE - SQL Server - Advanced Data Security (ADS) - ADS is now Azure Defender (Ticket 12112)
Jan 28, 2021	1.3.0	DELETE - Multiple in SQL Server - Advanced Data Security (ADS) section (Ticket 12125)

Jan 28, 2021	1.3.0	UPDATE - Multiple in 4.2 SQL Server - Advanced Data Security (ADS) section (Ticket 12126)
Aug 22, 2019	1.2.0	DELETE- Ensure that Azure Active Directory Admin is configured - Duplicate (Ticket 8018)
Sep 8, 2019	1.2.0	Added Azure Command Line Interface 2.0 commands (Ticket 7994)
May 18, 2020	1.2.0	UPDATE - Ensure that 'HTTP Version' is the latest, if used to run the web app - Typo in Audit procedure (Ticket 8628)
May 18, 2020	1.2.0	UPDATE - Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service - Incorrect Remediation Procedure (Ticket 8942)
May 18, 2020	1.2.0	Update - Ensure web app redirects all HTTP traffic to HTTPS in Azure App Service - Typo in Audit Procedure (Ticket 8943)
May 18, 2020	1.2.0	UPDATE - Ensure App Service Authentication is set on Azure App Service - remediation CLI correction (Ticket 8957)
Jun 2, 2020	1.2.0	UPDATE - Ensure that multi-factor authentication is enabled for all privileged users - Add reference (Ticket 10368)
Jun 2, 2020	1.2.0	UPDATE - Ensure that multi-factor authentication is enabled for all non-privileged users - Add reference (Ticket 10369)
Jun 2, 2020	1.2.0	UPDATE - Ensure that there are no guest users - Add reference guest user delete (Ticket 10370)
Jun 2, 2020	1.2.0	UPDATE - Ensure that 'Number of methods required to reset' is set to '2' - Add reference (Ticket 10374)
Jun 12, 2020	1.2.0	UPDATE - Ensure that 'Guest user permissions are limited' is set to 'Yes' - add reference (Ticket 10395)
Jun 12, 2020	1.2.0	UPDATE - Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to "0" - add reference (Ticket 10375)
Jun 12, 2020	1.2.0	UPDATE - Ensure that 'Notify users on password resets?' is set to 'Yes' - Add reference (Ticket 10376)

Jun 12, 2020	1.2.0	UPDATE - Ensure that 'Notify all admins when other admins reset their password?' is set to 'Yes' - Add reference (Ticket 10377)
Jun 12, 2020	1.2.0	UPDATE - Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No' - add reference (Ticket 10382)
Jun 12, 2020	1.2.0	UPDATE - Ensure that 'Users can register applications' is set to 'No' - add reference (Ticket 10394)
Jun 12, 2020	1.2.0	UPDATE - Ensure that 'Secure transfer required' is set to 'Enabled' - add reference (Ticket 10272)
Aug 21, 2020	1.2.0	UPDATE - Ensure that multi-factor authentication is enabled for all privileged users - Change in AAD Settings Location for Users and Groups (Ticket 11196)
Aug 21, 2020	1.2.0	UPDATE - Multiple - Audit and remediation instructions have changed 1.12, 1.13, 1.14 (Ticket 10504)
Aug 24, 2020	1.2.0	UPDATE - Mutiple - Add step in audit and remediation for change in GUI (Ticket 11288)
Aug 24, 2020	1.2.0	UPDATE - Ensure that 'Require Multi-Factor Auth to join devices' is set to 'Yes' - GUI changes for Audit and remediation (Ticket 11292)
Aug 24, 2020	1.2.0	UPDATE - Ensure that 'Automatic provisioning of monitoring agent' is set to 'On' - Remediation procedures has moved location (Ticket 11197)
Aug 24, 2020	1.2.0	UPDATE - Ensure Storage logging is enabled for Queue service for read, write, and delete requests - Modify reference (Ticket 10275)
Aug 24, 2020	1.2.0	UPDATE - Ensure Storage logging is enabled for Queue service for read, write, and delete requests - Modify Audit Procedure and Remediation Procedure wording (Ticket 10277)
Aug 24, 2020	1.2.0	UPDATE - Ensure that ADS - 'Advanced Threat Protection types' (ATP) is set to 'All' - Edit reference (Ticket 10304)
Aug 24, 2020	1.2.0	UPDATE - Ensure that 'Restrict user ability to access groups features in the Access Panel' is set to 'No' - Change Audit, Remeditation Procedure (Ticket 10397)

Aug 24, 2020	1.2.0	UPDATE - Ensure that 'Users can create security groups' is set to 'No' - Edit Audit Procedure, Remedation Procedure (Ticket 10398)
Aug 26, 2020	1.2.0	UPDATE - Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server - invalid reference (Ticket 10330)
Aug 26, 2020	1.2.0	UPDATE - Ensure 'Enforce SSL connection' is set to 'ENABLED' for MySQL Database Server - Add reference (Ticket 10331)
Aug 26, 2020	1.2.0	UPDATE - Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server - Add referenced (Ticket 10332)
Aug 26, 2020	1.2.0	UPDATE - Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server - Add reference (Ticket 10333)
Aug 26, 2020	1.2.0	UPDATE - Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server - Add reference (Ticket 10334)
Aug 26, 2020	1.2.0	UPDATE - Ensure server parameter 'log_duration' is set to 'ON' for PostgreSQL Database Server - Add reference (Ticket 10335)
Aug 26, 2020	1.2.0	UPDATE - Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server - Add reference (Ticket 10337)
Aug 26, 2020	1.2.0	UPDATE - Ensure server parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server - Add reference (Ticket 10339)
Aug 26, 2020	1.2.0	UPDATE - Ensure that 'OS disk' are encrypted - Edit reference (Ticket 10264)
Aug 26, 2020	1.2.0	UPDATE - Ensure that 'OS disk' are encrypted - Add Remediation Procedures (Ticket 10265)
Aug 26, 2020	1.2.0	UPDATE - Ensure that 'Data disks' are encrypted - Edit reference (Ticket 10266)
Aug 26, 2020	1.2.0	UPDATE - Ensure that 'Data disks' are encrypted - Add Remediation Procedures (Ticket 10267)

Aug 26, 2020	1.2.0	UPDATE - Ensure that 'Unattached disks' are encrypted - Edit reference (Ticket 10269)
Aug 27, 2020	1.2.0	DELETE - Ensure that 'Enable "All Users" group' is set to 'Yes' - Request to delete recommendation (Ticket 10401)
Sep 10, 2020	1.2.0	ADD - MULTIPLE - SQL Advanced Data Security related controls (Ticket 9081)
Sep 22, 2020	1.2.0	ADD - Ensure soft delete is enabled for Azure Storage (Ticket 11450)
Sep 22, 2020	1.2.0	DELETE - Ensure that 'AuditActionGroups' in 'auditing' policy for a SQL server is set properly (Ticket 11229)
Sep 22, 2020	1.2.0	UPDATE - Ensure that ADS - ATP 'Email service and co-administrators' is 'Enabled' - Modify term (Ticket 10310)
Sep 22, 2020	1.2.0	UPDATE - Ensure SQL server's TDE protector is encrypted with BYOK (Use your own key) - Change the expression 'Use Your own key' (Ticket 10341)
Sep 22, 2020	1.2.0	ADD - Ensure that Diagnostic Logs are enabled for all services which support it. (Ticket 11453)
Sep 24, 2020	1.2.0	UPDATE - Ensure that the expiration date is set on all keys - additional permissions required to automate this policy/rule (Ticket 8228)
Sep 24, 2020	1.2.0	Add Remediation - Ensure that UDP Services are restricted from the Internet (Ticket 10271)
Oct 7, 2020	1.2.0	UPDATE - Ensure that there are no guest users - Azure Command Line Interface 2.0 doesn't work as expected. (Ticket 11376)
Oct 7, 2020	1.2.0	UPDATE - Ensure that shared access signature tokens expire within an hour - Remediation Procedure 3.4 Ensure that shared access signature tokens expire within an hour (Ticket 10278)
Oct 7, 2020	1.2.0	UPDATE - Ensure that storage account access keys are periodically regenerated - add reference (Ticket 10273)

Oct 7, 2020	1.2.0	UPDATE - Ensure that storage account access keys are periodically regenerated - Add Remediation Procedure (Ticket 10274)
Oct 13, 2020	1.2.0	Update - Ensure that storage account access keys are periodically regenerated - change az cli command in audit procedure (Ticket 7995)
Oct 13, 2020	1.2.0	UPDATE - Ensure guest users are reviewed on a monthly basis - added PowerShell Check in audit (Ticket 11475)
Oct 13, 2020	1.2.0	DELETE - Ensure that security contact 'Phone number' is set (Ticket 11228)
Oct 13, 2020	1.2.0	UPDATE - Ensure that 'Users can create Microsoft 365 groups in Azure Portals' is set to 'No' - Replace 'Office 365' with 'Microsoft 365' and update references. (Ticket 11363)
Oct 13, 2020	1.2.0	DELETE - Ensure that 'Users who can manage Office 365 groups' is set to 'None' (Ticket 10400)
Oct 13, 2020	1.2.0	ADD - Ensure FTP deployments are disabled (Ticket 10503)
Oct 13, 2020	1.2.0	UPDATE - Ensure that no custom subscription owner roles are created - PowerShell Check (Ticket 11479)
Oct 14, 2020	1.2.0	Add - Ensure any of the ASC Default policy setting is not set to "Disabled" - Consolidate recommendations (Ticket 8791)
Oct 14, 2020	1.2.0	new not scored recommendations : Threat Detection Integration (Ticket 9047)
Oct 15, 2020	1.2.0	ADD - Ensure Security Defaults is enabled on Azure Active Directory (Ticket 11293)
Oct 15, 2020	1.2.0	ADD - Ensure storage for critical data are encrypted with Customer Managed Key (Ticket 10279)
Oct 15, 2020	1.2.0	UPDATE - Ensure that 'Users who can manage security groups' is set to 'None' - Change to wording (Owners can manage group membership requests in the Access Panel) (Ticket 10399)

Oct 15, 2020	1.2.0	UPDATE - Ensure that there are no guest users - Ensure that all Guest users are reviewed regularly rather than say they are not permitted (Ticket 10897)
Oct 15, 2020	1.2.0	ADD - subsections in Database Services section - Creating Subsections for better separation and ease for the end user (Ticket 9091)
Oct 15, 2020	1.2.0	DELETE - Ensure that shared access signature tokens are allowed only over https - This appears to be mitigated by 3.1. (Ticket 8711)
Oct 15, 2020	1.2.0	UPDATE - Ensure that Network Watcher is 'Enabled' - Info outdated in the recommendation. (Ticket 11559)
Oct 15, 2020	1.2.0	UPDATE - Ensure that Network Watcher is 'Enabled' - CLI Audit command does not list disabled regions. (Ticket 10906)
Oct 15, 2020	1.2.0	DELETE - Ensure that Activity Log Alert exists for Update Security Policy (Ticket 7706)
Oct 19, 2020	1.2.0	UPDATE - Ensure that standard pricing tier enabled for Virtual Machines - Add PowerShell Check (Ticket 11480)
Oct 19, 2020	1.2.0	UPDATE - Ensure that standard pricing tier enabled for PaaS SQL servers - Add PowerShell Check (Ticket 11481)
Oct 19, 2020	1.2.0	UPDATE - Ensure that standard pricing tier enabled for App Service - Add PowerShell Check (Ticket 11482)
Oct 19, 2020	1.2.0	UPDATE - Ensure that standard pricing tier enabled for Storage Accounts - Add PowerShell Check (Ticket 11483)
Oct 19, 2020	1.2.0	UDATE - Ensure that 'Automatic provisioning of monitoring agent' is set to 'On' - Add PowerShell Check (Ticket 11484)
Oct 19, 2020	1.2.0	UPDATE - Ensure any of the ASC Default policy setting is not set to "Disabled" - Audit procedure for section 2.8 produces misleading results (Ticket 9196)
Oct 20, 2020	1.2.0	UPDATE - Ensure that Advanced Data Security (ADS) and Advanced Threat Protection (ATP) on a SQL server is set to 'On' - Edit reference (Ticket 10303)

Oct 21, 2020	1.2.0	UPDATE - Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No' - add PowerShell check (Ticket 11477)
Oct 21, 2020	1.2.0	UPDATE - Ensure that 'Users can register applications' is set to 'No' - Add PowerShell Check (Ticket 11478)
Oct 21, 2020	1.2.0	ADD - Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled (Ticket 11451)
Oct 22, 2020	1.2.0	UPDATE - Ensure that Activity Log Alert exists for Delete Security Solution - fix the category of the metric rule for delete Security Solution (Ticket 11510)
Oct 22, 2020	1.2.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update Security Solution - fix the category of the metric rule for Create or Update Security Solution (Ticket 11511)
Oct 22, 2020	1.2.0	UPDATE - Ensure that 'Security contact emails' is set - Setting location change and renamed within Azure Portal (Ticket 11561)
Oct 22, 2020	1.2.0	UPDATE - Ensure that 'Send email notification for high severity alerts' is set to 'On' - Settings location and naming convention change in Azure Portal (Ticket 11562)
Oct 22, 2020	1.2.0	UPDATE - Ensure that 'Send email also to subscription owners' is set to 'On' - setting location and name change in Azure Portal (Ticket 11563)
Oct 22, 2020	1.2.0	ADD - Ensure Storage logging is enabled for Blob service for read, write, and delete requests (Ticket 11564)
Oct 22, 2020	1.2.0	ADD - Ensure Storage logging is enabled for Table service for read, write, and delete requests (Ticket 11565)
Oct 22, 2020	1.2.0	UPDATE - Multiple recommendations in section 5.2 - add UI remediation steps (Ticket 11554)
Oct 22, 2020	1.2.0	REMOVE - Log activity for all regions - This may no longer be valid if log settings is going away (Ticket 11583)
Oct 22, 2020	1.2.0	REMOVE - activity log to 365 days - No equivalent to this under Diagnostics settings (Ticket 11582)

Oct 22, 2020	1.2.0	Add UI steps to configuring Storage Profile (Ticket 8225)
Oct 22, 2020	1.2.0	ADD - Ensure Virtual Machines are utilizing Managed Disks (Ticket 11568)
Oct 22, 2020	1.2.0	UPDATE - Log profile recommendations should include recommendations for exporting to event hub (Ticket 9524)
Oct 22, 2020	1.2.0	UPDATE - Log profiles are being replaced with diagnostic settings for activity logs (Ticket 9523)
Oct 22, 2020	1.2.0	UPDATE - Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' - Console option location not up to date (Ticket 11598)
Oct 22, 2020	1.2.0	UPDATE - Ensure that 'PHP version' is the latest, if used to run the web app - Console location not up to date (Ticket 11600)
Oct 22, 2020	1.2.0	UPDATE - Ensure that 'HTTP Version' is the latest, if used to run the web app - Console location not up to date (Ticket 11601)
Oct 22, 2020	1.2.0	ADD - Ensure that 'OS and Data' disks are encrypted (replace OS and Data individual recommendations) (Ticket 11595)
Oct 23, 2020	1.2.0	UPDATE - Ensure that 'Unattached disks' are encrypted - Azure CIS 7.1-7.3 Guideline needs to be revisited in all aspects (Ticket 11342)
Oct 26, 2020	1.2.0	UPDATE - Ensure that Azure Defender is set to On for Virtual Machines - Virtual Machines changed to Servers (Ticket 11617)
Oct 26, 2020	1.2.0	ADD - recommendations for Azure Defender for all resource types (Ticket 8866)
Oct 27, 2020	1.2.0	UPDATE - Multiple Security Center Resource Recommendations - Azure Security Center standard tier is now called 'Azure Defender' (Ticket 11537)
Oct 31, 2020	1.2.0	ADD - Ensure Custom Role is assigned for Administering Resource Locks - Recommend creating an RBAC role to administer Resource locks (Ticket 8790)
Date	Version	Changes for this version Ticket #

2/15/2019	1.1.0	DELETE - 3.2 and 3.6 - Ensure that 'Storage... - Rules are no longer valid or do not require	6185
2/15/2019	1.1.0	UPDATE - 2.17 Ensure that security contact - Not digitally signed warning	6224
2/15/2019	1.1.0	UPDATE - 5.1.2 Ensure that Activity Log... - Retention Days set to 0 to allow indefinite retention	6559
2/15/2019	1.1.0	UPDATE - 2.14 - Security Policy option name 'SQL auditing & Threat detection' is longer valid	6560
2/15/2019	1.1.0	UPDATE - Ensure audit profile captures all the activities - Remediation CLI change	6705
2/15/2019	1.1.0	UPDATE - Ensure log profile captures activity...- audit and remediation steps	6706
2/15/2019	1.1.0	UPDATE - 8.4 Keyvault is recoverable - audit and remediation CLI update	6737
2/15/2019	1.1.0	DELETE - Section 4.2 - Redundancy of Controls when intent has already addressed in 4.1	6778
2/15/2019	1.1.0	ADD - SQL Servers (4.1): Ensure that Audit Action Group in auditing policy for a server is set properly	6779
2/15/2019	1.1.0	UPDATE - Section 4: All recommendations change Azure Portal/Console Audit and Remediation Steps except 4.1.9 and 4.1.10	6781
2/15/2019	1.1.0	UPDATE - 4.1.2 thru 4.1.7 - Changes required in Level and/or Scoring	6789
2/15/2019	1.1.0	UPDATE - 4.1.1 Ensure that 'Auditing' is set to 'On' (SQL Server) - Description and notes updated	6790
2/15/2019	1.1.0	UPDATE - 4.2.6 `TDE' on Database - Clarified wording and implementation process	6795
2/15/2019	1.1.0	UPDATE - 4.1.6 `Email Service and co-Administrators' - Update Default value	6796
2/15/2019	1.1.0	DELETE - 7.1 Ensure that VM agent is installed	6802
2/15/2019	1.1.0	UPDATE - 6.3 SQL server Firewall Policy - does 0.0.0.0 means public access or Azure IP range	6803
2/15/2019	1.1.0	UPDATE - 6.3 SQL server Firewall Policy can be overridden by DB Firewall policy	6804
2/15/2019	1.1.0	UPDATE - 2.12 - JIT Network Access - Not a free service - Making it Level 2 to be aligned with 2.1 Pricing tier `Standard`	6810

2/15/2019	1.1.0	UPDATE - 2.13 Adaptive Application Controls - Making it Level 2 to be aligned with 2.1 Pricing tier `Standard`	6811
2/15/2019	1.1.0	DELETE - 3.6 Ensure that 'Storage service encryption' is set to Enabled for File Service	6812
2/15/2019	1.1.0	UPDATE - 4.8 Threat Detection Retention - Add case 0 : Indefinite Retention	6813
2/15/2019	1.1.0	UPDATE - Ensure that Activity Log Alert exists for Create or Update or Delete...-title/rationale/description changed	6850
2/15/2019	1.1.0	DELETE - Ensure that Activity Log Alert exists for Delete SQL Server...5.2.9	6851
2/15/2019	1.1.0	ADD - Ensure that 'Unattached disks' are encrypted	6871
2/15/2019	1.1.0	UPDATE - Azure Security Center: Audit and Remediation console procedure changed	6874
2/15/2019	1.1.0	UPDATE - Ensure that the expiration date is set on all keys - Audit & Remediation Update	6920
2/15/2019	1.1.0	UPDATE - Ensure that the expiration date is set on all Secrets - Audit & Remediation Update	6921
2/15/2019	1.1.0	ADD - Propose 'Ensure 'Trusted Microsoft Services' is enabled for Storage Account access'	7079
2/15/2019	1.1.0	UPDATE- Ensure that 'Auditing' Retention is 'greater than 90 days' - Audit & Remediation Steps Update	7245
2/15/2019	1.1.0	ADD - Section for App Services Recommendations	7401
2/15/2019	1.1.0	UPDATE - Ensure that 'Members can invite' is set to 'No' - wording fix for Rationale	7407
2/15/2019	1.1.0	UPDATE - Section 2 - Azure Security Center changes to audit and remediation in all recommendations	7479
2/15/2019	1.1.0	UPDATE - SQL Service - Rename Section to Database Services	7559
2/15/2019	1.1.0	ADD - Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database	7566
2/15/2019	1.1.0	ADD - Ensure 'Enforce SSL connection' is set to 'ENABLED' for MySQL Database Server	7567
2/15/2019	1.1.0	ADD - Ensure server parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server	7572
2/15/2019	1.1.0	ADD - Ensure server parameter 'log_connections' is set to 'ON' for Azure Database for PostgreSQL server	7573
2/15/2019	1.1.0	ADD - Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server	7575

2/15/2019	1.1.0	ADD - Ensure server parameter 'log_duration' is set to 'ON' for PostgreSQL Database Server	7576
2/15/2019	1.1.0	ADD - Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server	7578
2/15/2019	1.1.0	ADD - Ensure server parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server	7579
2/15/2019	1.1.0	UPDATE - Section 1 - Multiple recommendations changed to Not Scored	7673
2/15/2019	1.1.0	UPDATE - 3.5 Ensure that shared access signature tokens are allowed only - scoring change	7687
2/15/2019	1.1.0	UPDATE - section 9 multiple recommendations - Scoring status changed to Not Scored	7688
2/15/2019	1.1.0	Update - mapping of V7 Critical Controls on all recommendations	7703
2/15/2019	1.1.0	UPDATE - Section 2 recommendations - Audit and Remediation Portal Steps (Edit setting -> Edit settings)	7741
2/15/2019	1.1.0	UPDATE - Ensure that 'Send email notification for high severity alerts' is - Update Title, Audit, Remediation steps	7742
2/15/2019	1.1.0	UPDATE - Ensure server parameter 'connection_throttling' is set to 'ON'... - updated rational	7878
2/15/2019	1.1.0	UPDATE - Monitoring using Activity Log Alerts - audit CLI : Remove GET GET	7880
2/15/2019	1.1.0	UPDATE - Section 5.2 - Update all Audit CLIs to filter out only desired alert rule	7932
2/15/2019	1.1.0	UPDATE - Section 4 multiple recommendations - changed to Advanced Data Security	7954
2/15/2019	1.1.0	UPDATE - Ensure ASC Default policy setting "Monitor System Updates" - Minor Correction in Audit Procedure	7993
2/20/2018	1.0.0	Initial Release	