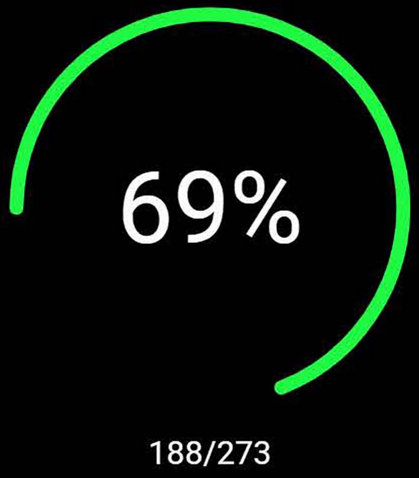
WhiteRook
Cyber

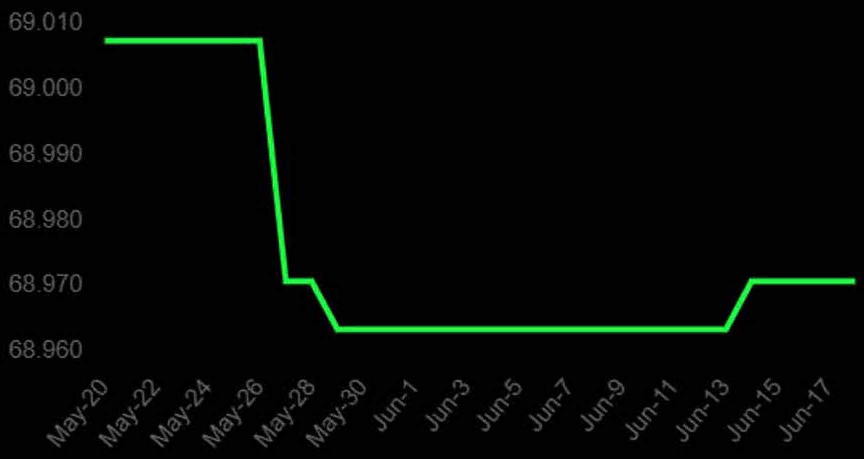
June 18, 2025

Sample Client
Cloud Assessment Report

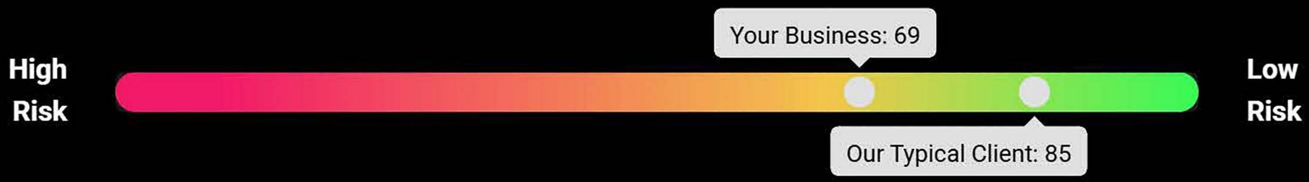
Executive Summary

Secure Score





The Secure Score is a reflection of your organization's security posture. It is a measure of how well your organization is leveraging the security features in Microsoft 365. The Secure Score is calculated based on the security features that you have enabled and the actions that you have taken to protect your organization. The higher the score, the more secure your organization is.



User Health

74 ✓

Total Users

The total number of users in the tenant. This includes all users, registered in Entra including unlicensed users, guest users, and service accounts.

4 ⓘ

Users have Global Administrator role

Global Administrators have full access to all administrative features in the tenant. It is recommended to have at least two global administrators to ensure that there is always a backup in case one administrator is unavailable. Excessive global administrators can increase the risk of unauthorized access to the tenant.

3 ⚠

Users without Multi-Factor Authentication

Multi-Factor Authentication (MFA) is a security feature that requires users to provide two or more verification factors to sign in to their account. Users without MFA are at a higher risk of unauthorized access to their account.

4 ⓘ

Users with weak Multi-Factor Authentication

Users with weak Multi-Factor Authentication (MFA) have MFA enabled, but are using weak authentication methods. Weak authentication methods include SMS, Voice, and Email. These methods are less secure than other MFA methods and can be more easily compromised.

0 ✓

Users with risky sign-ins

Risky users are users who have had risky sign-ins. Risky sign-ins can indicate that a user's account has been compromised or is at risk of being compromised. It is important to review risky users and take action to secure their accounts.

Device Health

18 ✓

Devices enrolled in Microsoft Entra

Entra is a device management solution that provides a single pane of glass for managing devices across multiple platforms.

0 ✓

Devices without encryption enabled

Devices without encryption enabled are at risk of data exposure due theft or loss.

1 ⚠

Devices that are not compliant with the organization's security policies

Devices that are not compliant with the organization's security policies are at risk of being compromised and should be investigated immediately.

8 ⓘ

Devices that have not been used in the last 30 days

Stale Devices are at greater risk of being compromised due to lack of security updates and patches and potential loss or theft.

Applications & Data

Default Sharing Policy

⚠ **Anyone**

By default, links are generated which can be accessed by anyone internal or external to the organization

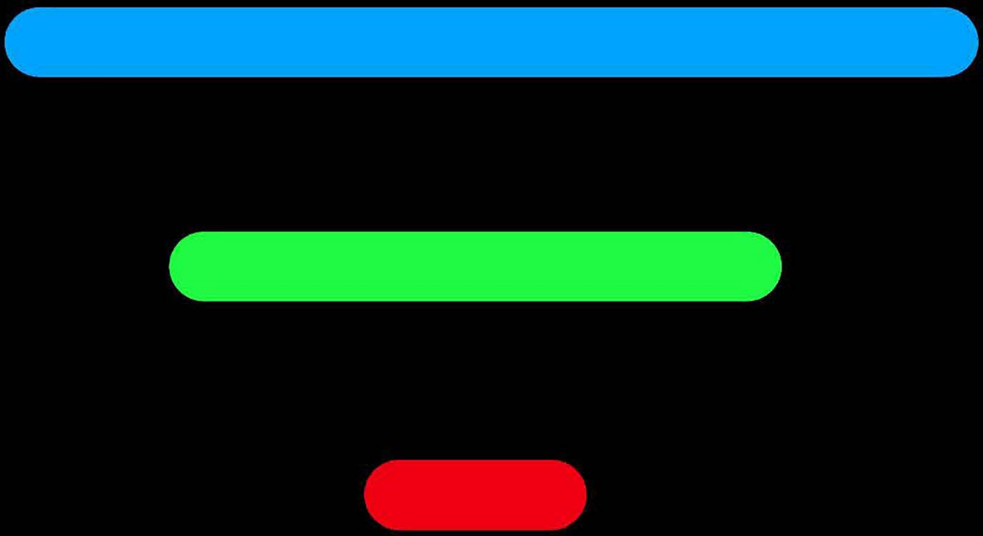
Email Health

[redacted] Domain	Yes Default	✓ SPF Check	✓ Verified	✗ DMARC - Missing
[redacted] Domain	No Default	⊖ SPF Check	⊖ Verified	⊖ DMARC

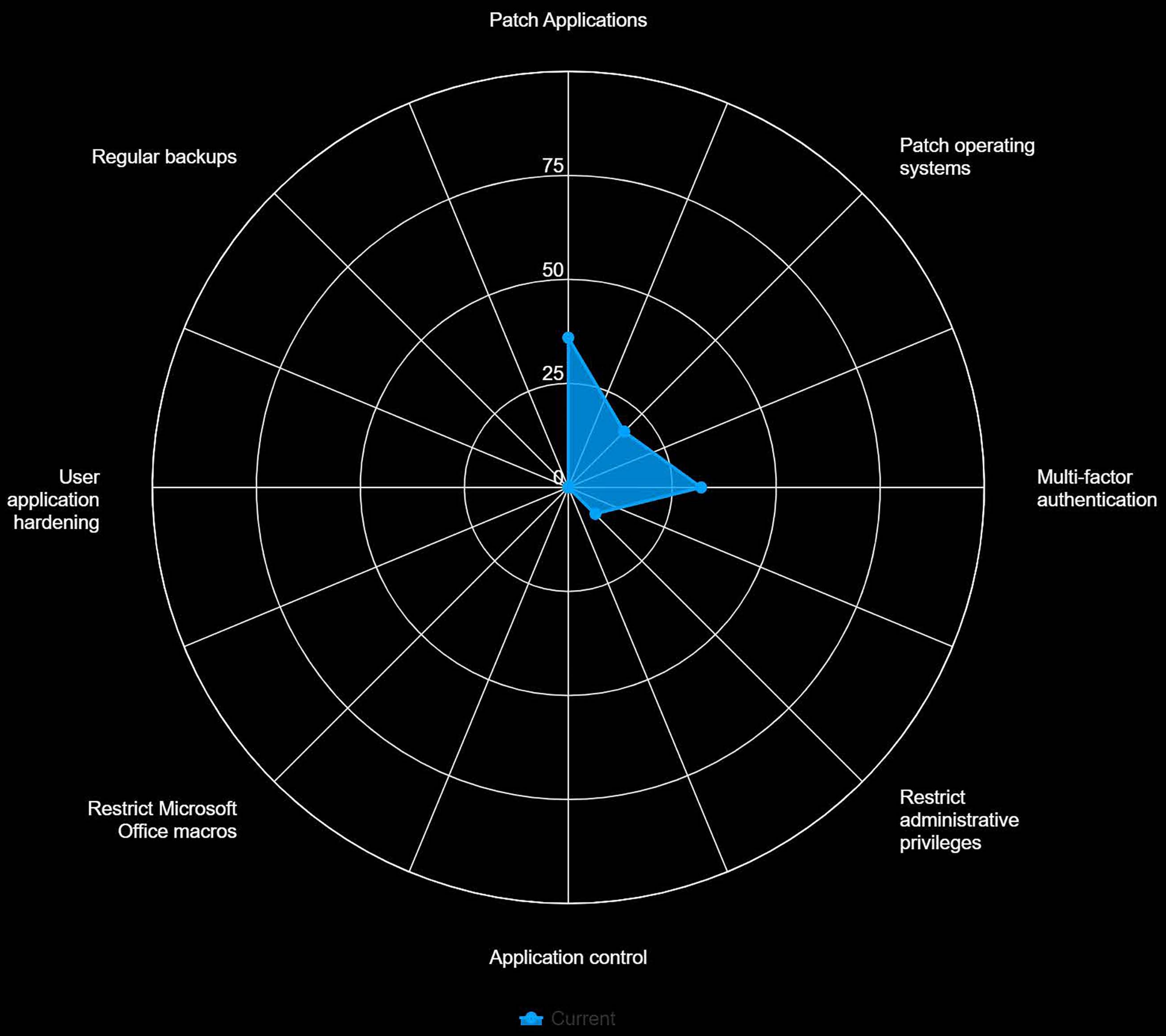
7,962
Emails Scanned

6,485
Emails Delivered

1,477
Emails Blocked



ACSC Essential Eight

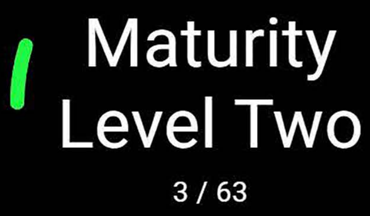


ACSC Essential Eight Overview

Maturity Level One

11 / 51

- ✓ 11 - Passed
- ✗ 19 - Failed
- ◎ 0 - Assumed Risk
- ○ 21 - Not Set



Maturity Level Two

3 / 63

- ✓ 3 - Passed
- ✗ 19 - Failed
- ◎ 0 - Assumed Risk
- ○ 41 - Not Set

Maturity Level Three

5 / 42

- ✓ 5 - Passed
- ✗ 12 - Failed
- ◎ 0 - Assumed Risk
- ○ 25 - Not Set

Exclude unset results

PA - Patch Applications

✗ **ML1-PA-01** - An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.

- ✗ Devices shall be enrolled for Defender for Business or Defender for Endpoint
  0 Devices found in defender

✗ **ML1-PA-02** - A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

- ✗ A Software Inventory is Actively Pulled from End User Devices
  No Software Inventory found

✗ **ML1-PA-03** - A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.

- ✗ A Software Inventory is Actively Pulled from End User Devices
  No Software Inventory found

✗ **ML1-PA-04** - A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

- ✗ A Software Inventory is Actively Pulled from End User Devices
  No Software Inventory found

○ **ML1-PA-05** - Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

- ○ Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
  Manual

✓ **ML1-PA-06** - Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

- ✓ Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
  No software with non-critical vulnerabilities older than 2 weeks found

✓ **ML1-PA-07** - Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release.

- ✓ Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
  No software with noncritical vulnerabilities older than 2 weeks found

○ **ML1-PA-08** - Online services that are no longer supported by vendors are removed.

○ Online services that are no longer supported by vendors are removed.
Manual

○ **ML1-PA-09** - Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.

○ Office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed
Manual

✗ **ML2-PA-01** - A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products.

✗ A Software Inventory is Actively Pulled from End User Devices
No Software Inventory found

✓ **ML2-PA-02** - Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.

✓ Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release.
No software with vulnerabilities older than 30 days found

✓ **ML3-PA-01** - Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

✓ Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
No software with critical vulnerabilities older than 48 hours found

✓ **ML3-PA-02** - Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

✓ Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
No software with noncritical vulnerabilities older than 2 weeks found

○ **ML3-PA-03** - Applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed.

PO - Patch operating systems

⊗ **ML1-PO-01** - An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.

- ⊗ Devices shall be enrolled for Defender for Business or Defender for Endpoint
  0 Devices found in defender

⊗ **ML1-PO-02** - A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

- ⊗ A Software Inventory is Actively Pulled from End User Devices
  No Software Inventory found

⊗ **ML1-PO-03** - A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.

- ⊗ A Software Inventory is Actively Pulled from End User Devices
  No Software Inventory found

⊗ **ML1-PO-04** - A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices.

- ⊗ A Software Inventory is Actively Pulled from End User Devices
  No Software Inventory found

○ **ML1-PO-05** - Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

- ○ Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist
  Manual

○ **ML1-PO-06** - Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.

- ○ Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist
  Manual

✓ **ML1-PO-07** - Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.

- ✓ Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.
  No software with vulnerabilities older than 30 days found

- ○ **ML1-PO-08** - Operating systems that are no longer supported by vendors are replaced.
  - ○ Operating systems that are no longer supported by vendors are replaced
    Manual
- ○ **ML3-PO-01** - A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.
  - ○ A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers.
    Manual
- ○ **ML3-PO-02** - A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware.
  - ○ A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware
    Manual
- ✓ **ML3-PO-03 -** Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
  - ✓ Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
    No software with critical vulnerabilities older than 48 hours found
- ✓ **ML3-PO-04 -** Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
  - ✓ Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.
    No software with vulnerabilities older than 30 days found
- ○ **ML3-PO-05** - Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.
  - ○ Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist
    Manual
- ○ **ML3-PO-06** - Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
  - ○ Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist
    Manual

○ **ML3-PO-07 -** Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist.

- ○ Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist
  Manual

⊗ **ML3-PO-08 -** The latest release, or the previous release, of operating systems are used.

- ⊗ The latest release, or the previous release, of operating systems are used.
  Devices found with out of date OS versions

MF - Multi-factor authentication

✓ **ML1-MF-01** - Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.

- ✓ MFA is enforced for all users
  Conditional Access Policy found that enables MFA for all users.

✓ **ML1-MF-02** - Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data

- ✓ MFA is enforced for all users
  Conditional Access Policy found that enables MFA for all users.

✓ **ML1-MF-03** - Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data.

- ✓ MFA is enforced for all users
  Conditional Access Policy found that enables MFA for all users.

○ **ML1-MF-04** - Multi-factor authentication is used to authenticate users to their organization's online customer services that process, store or communicate their organization's sensitive customer data.

- ○ Multi-factor authentication is used to authenticate users to their organization's online customer services that process, store or communicate their organization's sensitive customer data.
  Manual

✓ **ML-MF-05** - Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organization's sensitive customer data.

- ✓ MFA is enforced for all users
  Conditional Access Policy found that enables MFA for all users.

○ **ML1-MF-06** - Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.

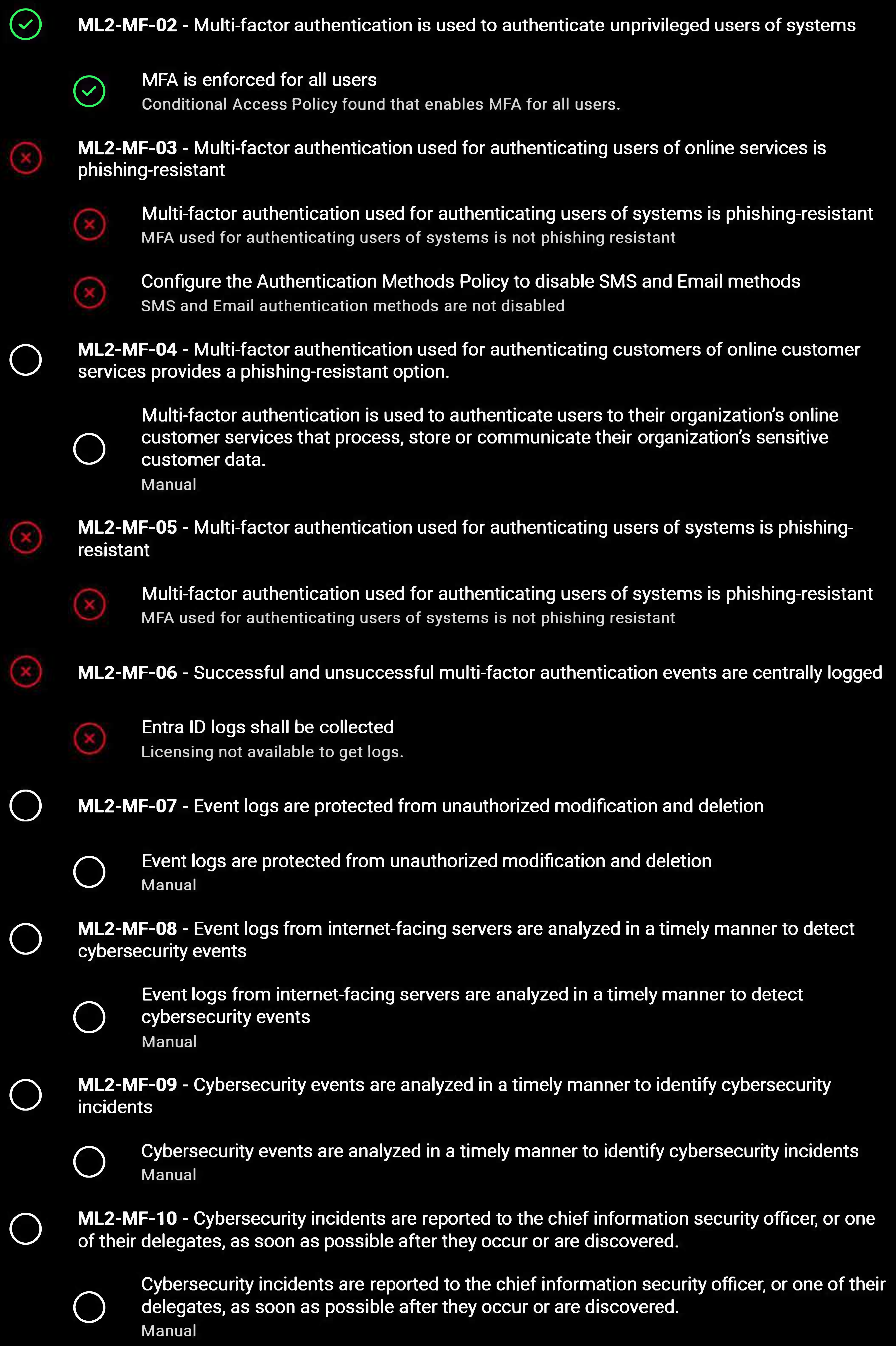
- ○ Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.
  Manual

✓ **ML1-MF-07** - Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or are

- ✓ MFA is enforced for all users
  Conditional Access Policy found that enables MFA for all users.

✓ **ML2-MF-01** - Multi-factor authentication is used to authenticate privileged users of systems

- ✓ MFA is enforced on accounts with highly privileged roles
  Conditional Access Policy found that is enforcing MFA for admins.



✓ **ML2-MF-02** - Multi-factor authentication is used to authenticate unprivileged users of systems

- ✓ MFA is enforced for all users
  Conditional Access Policy found that enables MFA for all users.

✗ **ML2-MF-03** - Multi-factor authentication used for authenticating users of online services is phishing-resistant

- ✗ Multi-factor authentication used for authenticating users of systems is phishing-resistant
  MFA used for authenticating users of systems is not phishing resistant
- ✗ Configure the Authentication Methods Policy to disable SMS and Email methods
  SMS and Email authentication methods are not disabled

○ **ML2-MF-04** - Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.

- ○ Multi-factor authentication is used to authenticate users to their organization’s online customer services that process, store or communicate their organization’s sensitive customer data.
  Manual

✗ **ML2-MF-05** - Multi-factor authentication used for authenticating users of systems is phishing-resistant

- ✗ Multi-factor authentication used for authenticating users of systems is phishing-resistant
  MFA used for authenticating users of systems is not phishing resistant

✗ **ML2-MF-06** - Successful and unsuccessful multi-factor authentication events are centrally logged

- ✗ Entra ID logs shall be collected
  Licensing not available to get logs.

○ **ML2-MF-07** - Event logs are protected from unauthorized modification and deletion

- ○ Event logs are protected from unauthorized modification and deletion
  Manual

○ **ML2-MF-08** - Event logs from internet-facing servers are analyzed in a timely manner to detect cybersecurity events

- ○ Event logs from internet-facing servers are analyzed in a timely manner to detect cybersecurity events
  Manual

○ **ML2-MF-09** - Cybersecurity events are analyzed in a timely manner to identify cybersecurity incidents

- ○ Cybersecurity events are analyzed in a timely manner to identify cybersecurity incidents
  Manual

○ **ML2-MF-10** - Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.

- ○ Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
  Manual

- ○ **ML2-MF-11** - Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered.
  - ○ Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered.
    Manual
- ○ **ML2-MF-12** - Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted.
  - ○ Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted.
    Manual
- ✓ **ML3-MF-01** - Multi-factor authentication is used to authenticate users of data repositories
  - ✓ MFA is enforced for all users
    Conditional Access Policy found that enables MFA for all users.
- ○ **ML3-MF-02** - Multi-factor authentication used for authenticating customers of online custmer services is phishing-resistant.
  - ○ Multi-factor authentication is used to authenticate users to their organization’s online customer services that process, store or communicate their organization’s sensitive customer data.
    Manual
- ✗ **ML3-MF-03** - Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.
  - ✗ Multi-factor authentication used for authenticating users of systems is phishing-resistant
    MFA used for authenticating users of systems is not phishing resistant
- ○ **ML3-MF-04** - Event logs from non-internet-facing servers are analyzed in a timely manner to detect cybersecurity events.
  - ○ Event logs from non-internet-facing servers are analyzed in a timely manner to detect cybersecurity events.
    Manual
- ○ **ML3-MF-05** - Event logs from workstations are analyzed in a timely manner to detect cybersecurity events
  - ○ Event logs from workstations are analyzed in a timely manner to detect cybersecurity events
    Manual

RA - Restrict administrative privileges

- ○ **ML1-RA-01** - Requests for privileged access to systems, applications and data repositories are validated when first requested
  - ○ Activation of privileged roles should be monitored and require approval
    Manual.
- ⊗ **ML1-RA-02** - Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
  - ✓ Highly privileged accounts shall be cloud-only
    All Global Admins are cloud-only.
  - ⊗ Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
    Global Admins exist with assigned licenses
- ⊗ **ML1-RA-03** - Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
  - ⊗ Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
    Global Admins exist with assigned licenses
- ✓ **ML1-RA-04 -** Privileged user accounts explicitly authorized to access online services are strictly limited to only what is required for users and services to undertake their duties.
  - ✓ Highly privileged accounts shall be cloud-only
    All Global Admins are cloud-only.
  - ✓ Ensure that between two and four global admins are designated
    4 Global admin were detected.
- ○ **ML1-RA-05** - Privileged users use separate privileged and unprivileged operating environments
  - ○ Privileged users use separate privileged and unprivileged operating environments
    Manual
  - ○ Local Administrator settings are configured for device joins
    Manual
- ○ **ML1-RA-06** - Unprivileged user accounts cannot logon to privileged operating environments
  - ○ Unprivileged user accounts cannot logon to privileged operating environments
    Manual
- ○ **ML1-RA-07** - Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments
  - ○ Privileged users use separate privileged and unprivileged operating environments
    Manual

- ○ **ML2-RA-01** - Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated
  - ○ Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated
    Manual
- ○ **ML2-RA-02** - Privileged access to systems and applications is disabled after 45 days of inactivity
  - ○ Privileged access to systems and applications is disabled after 45 days of inactivity
    Manual
- ○ **ML2-RA-03** - Privileged operating environments are not virtualized within unprivileged operating environments.
  - ○ Privileged operating environments are not virtualized within unprivileged operating environments.
    Manual
- ○ **ML2-RA-04** - Administrative activities are conducted through jump servers.
  - ○ Administrative activities are conducted through jump servers.
    Manual
- ○ **ML2-RA-05** - Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.
  - ○ Break Glass users are created for emergency access
    Manual.
  - ○ Local Administrator settings are configured for device joins
    Manual
  - ○ Enable Microsoft Entra Local Administrator Password Solution (LAPS)
    Manual
- ⊗ **ML2-RA-06** - Privileged access events are centrally logged.
  - ⊗ Entra ID logs shall be collected
    Licensing not available to get logs.
- ⊗ **ML2-RA-07** - Privileged user account and security group management events are centrally logged.
  - ⊗ Entra ID logs shall be collected
    Licensing not available to get logs.
- ○ **ML2-RA-08** - Event logs are protected from unauthorized modification and deletion.
  - ○ Event logs are protected from unauthorized modification and deletion
    Manual

○ **ML2-RA-09** - Event logs from internet-facing servers are analyzed in a timely manner to detect cybersecurity events.

- ○ Event logs from internet-facing servers are analyzed in a timely manner to detect cybersecurity events
  Manual

○ **ML2-RA-10** - Cybersecurity events are analyzed in a timely manner to identify cybersecurity incidents.

- ○ Cybersecurity events are analyzed in a timely manner to identify cybersecurity incidents
  Manual

○ **ML2-RA-11** - Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.

- ○ Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
  Manual

○ **ML2-RA-13** - Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered

- ○ Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered.
  Manual

○ **ML2-RA-14** - Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted.

- ○ Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted.
  Manual

○ **ML3-RA-01** - Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties.

- ○ Users assigned highly privileged roles shall not have permanent permissions
  Not Set

○ **ML3-RA-02** - Secure Admin Workstations are used in the performance of administrative activities

- ○ Privileged users use separate privileged and unprivileged operating environments
  Manual

○ **ML3-RA-03** - Just-in-time administration is used for administering systems and applications.

- ○ Users assigned highly privileged roles shall not have permanent permissions
  Not Set

○ **ML3-RA-04** - Memory integrity functionality is enabled.

- ○ Memory integrity functionality is enabled
  Manual

○ **ML3-RA-05** - Local Security Authority protection functionality is enabled

- ○ Local Security Authority protection functionality is enabled
  Manual

⊗ **ML3-RA-06** - Credential Guard functionality is enabled

- ⊗ Credential Guard functionality is enabled
  Credential Guard functionality is not enabled

⊗ **ML3-RA-07** - Remote Credential Guard functionality is enabled

- ⊗ Remote Credential Guard Functionality in Enabled
  Remote Credential Guard functionality is not enabled

○ **ML3-RA-08** - Event logs from non-internet-facing servers are analyzed in a timely manner to detect cybersecurity events

- ○ Event logs from non-internet-facing servers are analyzed in a timely manner to detect cybersecurity events.
  Manual

○ **ML3-RA-09** - Event logs from workstations are analyzed in a timely manner to detect cybersecurity events.

- ○ Event logs from workstations are analyzed in a timely manner to detect cybersecurity events
  Manual

AC - Application control

⊗ **ML1-AC-01** - Application control is implemented on workstations

⊗ Application control for Business is implemented on workstations
Application Control is not implemented on workstations

⊗ **ML1-AC-02** - Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients

⊗ Application control for Business is implemented on workstations
Application Control is not implemented on workstations

⊗ **ML1-AC-03** - Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organization-approved set

⊗ Application control for Business is implemented on workstations
Application Control is not implemented on workstations

○ **ML2-AC-01** - Application control is implemented on internet-facing servers.

○ Application control is implemented on servers.
Manual

⊗ **ML2-AC-02** - Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients

⊗ Application control for Business is implemented on workstations
Application Control is not implemented on workstations

⊗ **ML2-AC-03** - Microsoft's recommended application blocklist is implemented

⊗ Application control for Business is implemented on workstations
Application Control is not implemented on workstations

○ **ML2-AC-04** - Application control rulesets are validated on an annual or more frequent basis.

○ Application control rulesets are validated on an annual or more frequent basis.
Manual

○ **ML2-AC-05** - Allowed and blocked application control events are centrally logged

○ Allowed and blocked application control events are centrally logged
Manual

○ **ML2-AC-06** - Event logs are protected from unauthorized modification and deletion

○ Event logs are protected from unauthorized modification and deletion
Manual

○ **ML2-AC-07** - Event logs from internet-facing servers are analyzed in a timely manner to detect cybersecurity events

- ○ Event logs from internet-facing servers are analyzed in a timely manner to detect cybersecurity events
  Manual

○ **ML2-AC-08** - Cybersecurity events are analyzed in a timely manner to identify cybersecurity incidents.

- ○ Cybersecurity events are analyzed in a timely manner to identify cybersecurity incidents
  Manual

○ **ML2-AC-09** - Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered

- ○ Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
  Manual

○ **ML2-AC-10** - Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered.

- ○ Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered.
  Manual

○ **ML2-AC-11** - Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted

- ○ Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted.
  Manual

○ **ML3-AC-01** - Application control is implemented on non-internet-facing servers

- ○ Application control is implemented on servers.
  Manual

⊗ **ML3-AC-02** - Application control restricts the execution of drivers to an organization-approved set

- ⊗ Application control for Business is implemented on workstations
  Application Control is not implemented on workstations

⊗ **ML3-AC-03** - Microsoft's vulnerable driver blocklist is implemented

- ⊗ Application control for Business is implemented on workstations
  Application Control is not implemented on workstations

○ **ML3-AC-04** - Event logs from non-internet-facing servers are analyzed in a timely manner to detect cybersecurity events

- ○ Event logs from non-internet-facing servers are analyzed in a timely manner to detect cybersecurity events.
  Manual

○ **ML3-AC-05** - Event logs from workstations are analyzed in a timely manner to detect cybersecurity events

- ○ Event logs from workstations are analyzed in a timely manner to detect cybersecurity events
  Manual

OM - Restrict Microsoft Office macros

⊗ **ML1-OM-01** - Microsoft Office macros are disabled for users that do not have a demonstrated business requirement

- ⊗ Microsoft Office macros are disabled for users that do not have a demonstrated business requirement
  Office Macros are not disabled for users without business requirement

⊗ **ML1-OM-02** - Microsoft Office macros in files originating from the internet are blocked

- ⊗ Microsoft Office macros in files originating from the internet are blocked
  Office Macros Originating from Internet are not blocked

⊗ **ML1-OM-03** - Microsoft Office macro antivirus scanning is enabled

- ⊗ Microsoft Office macro antivirus scanning is enabled
  Office Macros Antivirus Scanning is not enabled

⊗ **ML1-OM-04** - Microsoft Office macro security settings cannot be changed by users

- ⊗ Microsoft Office macro security settings can't be changed by users
  Users can change macro security settings

⊗ **ML2-OM-01** - Microsoft Office macros are blocked from making Win32 API calls

- ⊗ Microsoft Office macros are blocked from making Win32 API calls
  Microsoft Office Macros are not blocked from making WIN32 API calls

⊗ **ML3-OM-01** - Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a trusted publisher are allowed to execute

- ⊗ Only Microsoft Office macros running from within a sandboxed environment, a Trusted Location or that are digitally signed by a Trusted Publisher are allowed to execute
  Macros can be run from untrusted locations

⊗ **ML3-OM-02** - Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations

- ⊗ Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.
  Non-privileged users can modify content in trusted locations

⊗ **ML3-OM-03** - Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations

- ⊗ Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.
  Non-privileged users can modify content in trusted locations

- ⊗ **ML3-OM-04** - Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View
  - ⊗ Microsoft Office macros digitally signed by an untrusted publisher can't be enabled via the Message Bar or Backstage View
    Office Macros from Untrusted Publisher can be enabled
- ⊗ **ML3-OM-05** - Microsoft Office macros digitally signed by signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View
  - ⊗ Microsoft Office macros digitally signed by an untrusted publisher can't be enabled via the Message Bar or Backstage View
    Office Macros from Untrusted Publisher can be enabled
- ○ **ML3-OM-06** - Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis
  - ○ Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis
    Manual

AH - User application hardening

⊗ **ML1-AH-01** - Internet Explorer 11 is disabled or removed

- ⊗ Internet Explorer 11 is disabled or removed
  Internet Explorer 11 is not disabled or removed

○ **ML1-AH-02** - Web browsers do not process Java from the internet

- ○ Web browsers do not process Java from the internet
  Manual

⊗ **ML1-AH-03** - Web browsers do not process web advertisements from the internet

- ⊗ Web browsers do not process web advertisements from the internet.
  Web browsers process web advertisements from the internet

○ **ML1-AH-04** - Web browser security settings cannot be changed by users

- ○ Microsoft Edge Policies are configured and enforced
  Manual

⊗ **ML2-AH-01** - Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur

- ⊗ Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur
  Web browsers are not hardened using ASD and vendor hardening guidance

⊗ **ML2-AH-02** - Microsoft Office is blocked from creating child processes

- ⊗ Microsoft Office is blocked from creating child processes
  Microsoft Office is not blocked from creating child processes

⊗ **ML2-AH-03** - Microsoft Office is blocked from creating executable content

- ⊗ Microsoft Office is blocked from creating executable content
  Microsoft Office is not blocked from creating executable content

⊗ **ML2-AH-04** - Microsoft Office is blocked from injecting code into other processes

- ⊗ Microsoft Office is blocked from injecting code into other processes
  Microsoft Office is not blocked from injecting code into other processes

⊗ **ML2-AH-05** - Microsoft Office is configured to prevent activation of Object Linking and Embedding packages

- ⊗ Microsoft Office is configured to prevent object linking and embedding packages
  Microsoft Office is not configured to prevent object linking and embedding packages

- ⊗ **ML2-AH-06** - Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur
  - ⊗ Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur
    Office Productivity Suites are not hardened using ASD and vendor hardening guidance
- ⊗ **ML2-AH-07** - Office productivity suite security settings cannot be changed by users
  - ⊗ Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur
    Office Productivity Suites are not hardened using ASD and vendor hardening guidance
- ⊗ **ML2-AH-08** - PDF software is blocked from creating child processes
  - ⊗ PDF software is blocked from creating child processes
    PDF Software is not blocked from creating child processes
- ⊗ **ML2-AH-09** - PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur
  - ⊗ PDF software is blocked from creating child processes
    PDF Software is not blocked from creating child processes
  - ○ Microsoft Edge Policies are configured and enforced
    Manual
- ⊗ **ML2-AH-10** - PDF software security settings cannot be changed by users
  - ○ Microsoft Edge Policies are configured and enforced
    Manual
  - ⊗ PDF software is blocked from creating child processes
    PDF Software is not blocked from creating child processes
- ○ **ML2-AH-11** - PowerShell module logging, script block logging and transcription events are centrally logged
  - ○ PowerShell module logging, script block logging and transcription events are centrally logged
    Manual
- ○ **ML2-AH-12** - Command line process creation events are centrally logged
  - ○ Command line process creation events are centrally logged
    Manual
- ○ **ML2-AH-13** - Event logs are protected from unauthorized modification and deletion
  - ○ Event logs are protected from unauthorized modification and deletion
    Manual

○ **ML2-AH-14 -** Event logs from internet-facing servers are analyzed in a timely manner to detect cybersecurity events

- ○ Event logs from internet-facing servers are analyzed in a timely manner to detect cybersecurity events
  Manual

○ **ML2-AH-15 -** Cybersecurity events are analyzed in a timely manner to identify cybersecurity incidents

- ○ Cybersecurity events are analyzed in a timely manner to identify cybersecurity incidents
  Manual

○ **ML2-AH-16 -** Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered

- ○ Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
  Manual

○ **ML2-AH-17 -** Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered

- ○ Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered.
  Manual

○ **ML2-AH-18 -** Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted

- ○ Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted.
  Manual

⊗ **ML3-AH-01 -** .NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed

- ⊗ .NET Framework and PowerShell 2.0 are disabled or removed
  .NET Framework and PowerShell 2.0 are not disabled or removed

⊗ **ML3-AH-02 -** Windows PowerShell 2.0 is disabled or removed

- ⊗ .NET Framework and PowerShell 2.0 are disabled or removed
  .NET Framework and PowerShell 2.0 are not disabled or removed

○ **ML3-AH-03 -** PowerShell is configured to use Constrained Language Mode

- ○ PowerShell is configured to use Constrained Language Mode
  Manual

○ **ML3-AH-04 -** Event logs from non-internet-facing servers are analyzed in a timely manner to detect cybersecurity events

- ○ Event logs from non-internet-facing servers are analyzed in a timely manner to detect cybersecurity events.
  Manual

○ **ML3-AH-05 -** Event logs from workstations are analyzed in a timely manner to detect cybersecurity events

- ○ Event logs from workstations are analyzed in a timely manner to detect cybersecurity events
  Manual

RB - Regular backups

- ○ **ML1-RB-01** - Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements
  - ○ Retention Policies shall be configured
    Manual
  - ○ Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements
    Manual
- ○ **ML1-RB-02** - Backups of data, applications and settings are synchronized to enable restoration to a common point in time.
  - ○ Backups of data, applications and settings are synchronized to enable restoration to a common point in time.
    Manual
- ○ **ML1-RB-03** - Backups of data, applications and settings are retained in a secure and resilient manner
  - ○ Backups of data, applications and settings are retained in a secure and resilient manner
    Manual
- ○ **ML1-RB-04 -** Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises
  - ○ Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
    Manual
- ○ **ML1-RB-05** - Unprivileged user accounts cannot access backups belonging to other user accounts
  - ○ Access to backups is restricted based on role and least privilege
    Manual
- ○ **ML1-RB-06** - Unprivileged user accounts are prevented from modifying and deleting backups
  - ○ Backups are protected from modification and deletion by all users, including administrators, during their defined retention period
    Manual
- ○ **ML2-RB-01** - Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts
  - ○ Access to backups is restricted based on role and least privilege
    Manual
- ○ **ML2-RB-02** - Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups
  - ○ Backups are protected from modification and deletion by all users, including administrators, during their defined retention period
    Manual

○ **ML3-RB-01** - Unprivileged user accounts cannot access their own backups

- ○ Access to backups is restricted based on role and least privilege
  Manual

○ **ML3-RB-02** - Privileged user accounts (excluding backup administrator accounts) cannot access their own backups

- ○ Access to backups is restricted based on role and least privilege
  Manual

○ **ML3-RB-03** - Backup administrator accounts are prevented from modifying and deleting backups during their retention period

- ○ Backups are protected from modification and deletion by all users, including administrators, during their defined retention period
  Manual