Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Essential Eight maturity model

First published: June 2017
Last updated: November 2023

Introduction

The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of the *Strategies to mitigate cyber security incidents*, to help organisations protect themselves against various cyber threats. The most effective of these mitigation strategies are the Essential Eight.

The Essential Eight has been designed to protect organisations' internet-connected information technology networks. While the principles behind the Essential Eight may be applied to enterprise mobility and operational technology networks, it was not designed for such purposes and alternative mitigation strategies may be more appropriate to defend against unique cyber threats to these environments.

The *Essential Eight maturity model*, first published in June 2017 and updated regularly, supports the implementation of the Essential Eight. It is based on ASD's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.

Implementation

When implementing the Essential Eight, organisations should identify and plan for a target maturity level suitable for their environment. Organisations should then progressively implement each maturity level until that target is achieved.

As the mitigation strategies that constitute the Essential Eight have been designed to complement each other, and to provide coverage of various cyber threats, organisations should plan their implementation to achieve the same maturity level across all eight mitigation strategies before moving onto higher maturity levels.

Organisations should implement the Essential Eight using a risk-based approach. In doing so, organisations should seek to minimise any exceptions and their scope, for example, by implementing compensating controls and ensuring the number of systems or users impacted are minimised. In addition, any exceptions should be documented and approved through an appropriate process. Subsequently, the need for any exceptions, and associated compensating controls, should be monitored and reviewed on a regular basis. Note, the appropriate use of exceptions should not preclude an organisation from being assessed as meeting the requirements for a given maturity level.

As the Essential Eight outlines a minimum set of preventative measures, organisations need to implement additional measures to those within this maturity model where it is warranted by their environment. Further, while the Essential Eight can help to mitigate the majority of cyber threats, it will not mitigate all cyber threats. As such, additional mitigation strategies and controls need to be considered, including those from the *Strategies to mitigate cyber security incidents* and the *Information security manual*.

Finally, there is no requirement for organisations to have their Essential Eight implementation certified by an independent party. However, Essential Eight implementations may need to be assessed by an independent party if required by a government directive or policy, by a regulatory authority, or as part of contractual arrangements.

Maturity levels

To assist organisations with their implementation of the Essential Eight, four maturity levels have been defined (Maturity Level Zero through to Maturity Level Three). With the exception of Maturity Level Zero, the maturity levels are based on mitigating increasing levels of tradecraft (i.e. tools, tactics, techniques and procedures) and targeting, which are discussed in more detail below. Depending on overall capability, malicious actors may exhibit different levels of tradecraft for different operations against different targets. For example, malicious actors capable of advanced tradecraft may use it against one target while using basic tradecraft against another. As such, organisations should consider what level of tradecraft and targeting, rather than which malicious actors, they are aiming to mitigate.

Organisations need to consider that the likelihood of being targeted is influenced by their desirability to malicious actors, and the consequences of a cyber security incident will depend on their requirement for the confidentiality of their data, as well as their requirement for the availability and integrity of their systems and data. This, in combination with the descriptions for each maturity level, can be used to help determine a target maturity level to implement.

Finally, Maturity Level Three will not stop malicious actors that are willing and able to invest enough time, money and effort to compromise a target. As such, organisations still need to consider the remainder of the mitigation strategies from the *Strategies to mitigate cyber security incidents* and the *Information security manual*.

Maturity Level Zero

This maturity level signifies that there are weaknesses in an organisation's overall cyber security posture. When exploited, these weaknesses could facilitate the compromise of the confidentiality of their data, or the integrity or availability of their systems and data, as described by the tradecraft and targeting in Maturity Level One below.

Maturity Level One

The focus of this maturity level is malicious actors who are content to simply leverage commodity tradecraft that is widely available in order to gain access to, and likely control of, a system. For example, malicious actors opportunistically using a publicly-available exploit for a vulnerability in an online service which had not been patched, or authenticating to an online service using credentials that were stolen, reused, brute forced or guessed.

Generally, malicious actors are looking for any victim rather than a specific victim and will opportunistically seek common weaknesses in many targets rather than investing heavily in gaining access to a specific target. Malicious actors will employ common social engineering techniques to trick users into weakening the security of a system and launch malicious applications. If user accounts that malicious actors compromise have special privileges they will exploit it. Depending on their intent, malicious actors may also destroy data (including backups).

Maturity Level Two

The focus of this maturity level is malicious actors operating with a modest step-up in capability from the previous maturity level. These malicious actors are willing to invest more time in a target and, perhaps more importantly, in the effectiveness of their tools. For example, these malicious actors will likely employ well-known tradecraft in order to better attempt to bypass controls implemented by a target and evade detection. This includes actively targeting credentials using phishing and employing technical and social engineering techniques to circumvent weak multi-factor authentication.

Generally, malicious actors are likely to be more selective in their targeting but still somewhat conservative in the time, money and effort they may invest in a target. Malicious actors will likely invest time to ensure their phishing is effective and employ common social engineering techniques to trick users to weaken the security of a system and launch malicious applications. If user accounts that malicious actors compromise have special privileges they will exploit it, otherwise they will seek user accounts with special privileges. Depending on their intent, malicious actors may also destroy all data (including backups) accessible to a user account with special privileges.

Maturity Level Three

The focus of this maturity level is malicious actors who are more adaptive and much less reliant on public tools and techniques. These malicious actors are able to exploit the opportunities provided by weaknesses in their target's cyber security posture, such as the existence of older software or inadequate logging and monitoring. Malicious actors do this to not only extend their access once initial access has been gained to a target, but to evade detection and solidify their presence. Malicious actors make swift use of exploits when they become publicly available as well as other tradecraft that can improve their chance of success.

Generally, malicious actors may be more focused on particular targets and, more importantly, are willing and able to invest some effort into circumventing the idiosyncrasies and particular policy and technical controls implemented by their targets. For example, this includes social engineering a user to not only open a malicious document but also to unknowingly assist in bypassing controls. This can also include circumventing stronger multi-factor authentication by stealing authentication token values to impersonate a user. Once a foothold is gained on a system, malicious actors will seek to gain privileged credentials or password hashes, pivot to other parts of a network, and cover their tracks. Depending on their intent, malicious actors may also destroy all data (including backups).

Requirements for each maturity level

Requirements for Maturity Level One through to Maturity Level Three are outlined in Appendices A to C. A comparison of the maturity levels, with changes between maturity levels indicated via bolded text, is outlined in Appendix D.

Further information

The *Essential Eight maturity model* is part of a suite of related publications:

- Answers to questions on this maturity model are available in the *Essential Eight maturity model FAQ* publication.
- Additional mitigation strategies are available in the *Strategies to mitigate cyber security incidents* publication.
- Further Information on patching activities is available in the *Patching applications and operating systems* publication.
- Further Information on implementing multi-factor authentication is available in the *Implementing multi-factor authentication* publication.
- Further Information on controlling privileged user accounts is available in the *Restricting administrator privileges* publication.
- Further Information on implementing application control is available in the *Implementing application control* publication.
- Further Information on controlling Microsoft Office macros is available in the *Restricting Microsoft Office macros* publication.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Appendix A: Maturity Level One

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	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.
	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 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.
	Online services 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.
Patch operating systems	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	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 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.

	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 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 workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.
	Operating systems that are no longer supported by vendors are replaced.
Multi-factor authentication	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.
	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.
	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.
	Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.
	Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.
	Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data.
	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.
Restrict administrative privileges	Requests for privileged access to systems, applications and data repositories are validated when first requested.
	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.

	Privileged users use separate privileged and unprivileged operating environments.
	Unprivileged user accounts cannot logon to privileged operating environments.
	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.
Application control	Application control is implemented on workstations.
	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
Restrict Microsoft Office macros	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.
	Microsoft Office macros in files originating from the internet are blocked.
	Microsoft Office macro antivirus scanning is enabled.
	Microsoft Office macro security settings cannot be changed by users.
User application hardening	Internet Explorer 11 is disabled or removed.
	Web browsers do not process Java from the internet.
	Web browsers do not process web advertisements from the internet.
	Web browser security settings cannot be changed by users.
Regular backups	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.
	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.
	Backups of data, applications and settings are retained in a secure and resilient manner.
	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
	Unprivileged user accounts cannot access backups belonging to other user accounts.
	Unprivileged user accounts are prevented from modifying and deleting backups.

Appendix B: Maturity Level Two

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	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 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.
	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 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.
	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.
	Online services 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.
Patch operating systems	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.

	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 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.
	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 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 workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release.
	Operating systems that are no longer supported by vendors are replaced.
Multi-factor authentication	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.
	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.
	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.
	Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.
	Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.
	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 privileged users of systems.
	Multi-factor authentication is used to authenticate unprivileged users of systems.
	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.

	Multi-factor authentication used for authenticating users of online services is phishing-resistant.
	Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.
	Multi-factor authentication used for authenticating users of systems is phishing-resistant.
	Successful and unsuccessful multi-factor authentication events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict administrative privileges	Requests for privileged access to systems, applications and data repositories are validated when first requested.
	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.
	Privileged access to systems and applications is disabled after 45 days of inactivity.
	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.
	Privileged users use separate privileged and unprivileged operating environments.
	Privileged operating environments are not virtualised within unprivileged operating environments.

	Unprivileged user accounts cannot logon to privileged operating environments.
	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.
	Administrative activities are conducted through jump servers.
	Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.
	Privileged access events are centrally logged.
	Privileged user account and security group management events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Application control	Application control is implemented on workstations.
	Application control is implemented on internet-facing servers.
	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
	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 restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
	Microsoft's recommended application blocklist is implemented.
	Application control rulesets are validated on an annual or more frequent basis.

	Allowed and blocked application control events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict Microsoft Office macros	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.
	Microsoft Office macros in files originating from the internet are blocked.
	Microsoft Office macro antivirus scanning is enabled.
	Microsoft Office macros are blocked from making Win32 API calls.
	Microsoft Office macro security settings cannot be changed by users.
User application hardening	Internet Explorer 11 is disabled or removed.
	Web browsers do not process Java from the internet.
	Web browsers do not process web advertisements from the internet.
	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	Web browser security settings cannot be changed by users.
	Microsoft Office is blocked from creating child processes.
	Microsoft Office is blocked from creating executable content.
	Microsoft Office is blocked from injecting code into other processes.
	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

	Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	Office productivity suite security settings cannot be changed by users.
	PDF software is blocked from creating child processes.
	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	PDF software security settings cannot be changed by users.
	PowerShell module logging, script block logging and transcription events are centrally logged.
	Command line process creation events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Regular backups	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.
	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.
	Backups of data, applications and settings are retained in a secure and resilient manner.
	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
	Unprivileged user accounts cannot access backups belonging to other user accounts.
	Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.

Unprivileged user accounts are prevented from modifying and deleting backups.
Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.

Appendix C: Maturity Level Three

Mitigation Strategy	Description
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	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 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.
	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 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 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 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 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.
	Online services 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.

	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.
Patch operating systems	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	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 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 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 firmware.
	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 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 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 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 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 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 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 one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.
	The latest release, or the previous release, of operating systems are used.
	Operating systems that are no longer supported by vendors are replaced.
Multi-factor authentication	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.
	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.
	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.
	Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.
	Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.
	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 privileged users of systems.
	Multi-factor authentication is used to authenticate unprivileged users of systems.
	Multi-factor authentication is used to authenticate users of data repositories.
	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.
	Multi-factor authentication used for authenticating users of online services is phishing-resistant.
	Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.

	Multi-factor authentication used for authenticating users of systems is phishing-resistant.
	Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.
	Successful and unsuccessful multi-factor authentication events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from workstations are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict administrative privileges	Requests for privileged access to systems, applications and data repositories are validated when first requested.
	Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated.
	Privileged access to systems and applications is disabled after 45 days of inactivity.
	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
	Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties.
	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.

Secure Admin Workstations are used in the performance of administrative activities.
Privileged users use separate privileged and unprivileged operating environments.
Privileged operating environments are not virtualised within unprivileged operating environments.
Unprivileged user accounts cannot logon to privileged operating environments.
Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.
Just-in-time administration is used for administering systems and applications.
Administrative activities are conducted through jump servers.
Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.
Memory integrity functionality is enabled.
Local Security Authority protection functionality is enabled.
Credential Guard functionality is enabled.
Remote Credential Guard functionality is enabled.
Privileged access events are centrally logged.
Privileged user account and security group management events are centrally logged.
Event logs are protected from unauthorised modification and deletion.
Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.
Event logs from workstations are analysed in a timely manner to detect cyber security events.
Cyber security events are analysed in a timely manner to identify cyber security incidents.
Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.

	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Application control	Application control is implemented on workstations.
	Application control is implemented on internet-facing servers.
	Application control is implemented on non-internet-facing servers.
	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
	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 restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
	Application control restricts the execution of drivers to an organisation-approved set.
	Microsoft's recommended application blocklist is implemented.
	Microsoft's vulnerable driver blocklist is implemented.
	Application control rulesets are validated on an annual or more frequent basis.
	Allowed and blocked application control events are centrally logged.
	Event logs are protected from unauthorised modification and deletion.
	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.
	Event logs from workstations are analysed in a timely manner to detect cyber security events.
	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.

	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict Microsoft Office macros	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.
	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.
	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.
	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 signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View.
	Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.
	Microsoft Office macros in files originating from the internet are blocked.
	Microsoft Office macro antivirus scanning is enabled.
	Microsoft Office macros are blocked from making Win32 API calls.
	Microsoft Office macro security settings cannot be changed by users.
User application hardening	Internet Explorer 11 is disabled or removed.
	Web browsers do not process Java from the internet.
	Web browsers do not process web advertisements from the internet.
	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	Web browser security settings cannot be changed by users.
	Microsoft Office is blocked from creating child processes.

Microsoft Office is blocked from creating executable content.
Microsoft Office is blocked from injecting code into other processes.
Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.
Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
Office productivity suite security settings cannot be changed by users.
PDF software is blocked from creating child processes.
PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
PDF software security settings cannot be changed by users.
.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.
Windows PowerShell 2.0 is disabled or removed.
PowerShell is configured to use Constrained Language Mode.
PowerShell module logging, script block logging and transcription events are centrally logged.
Command line process creation events are centrally logged.
Event logs are protected from unauthorised modification and deletion.
Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.
Event logs from workstations are analysed in a timely manner to detect cyber security events.
Cyber security events are analysed in a timely manner to identify cyber security incidents.
Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.

	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Regular backups	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.
	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.
	Backups of data, applications and settings are retained in a secure and resilient manner.
	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
	Unprivileged user accounts cannot access backups belonging to other user accounts.
	Unprivileged user accounts cannot access their own backups.
	Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.
	Privileged user accounts (excluding backup administrator accounts) cannot access their own backups.
	Unprivileged accounts are prevented from modifying and deleting backups.
	Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.
	Backup administrator accounts are prevented from modifying and deleting backups during their retention period.

Appendix D: Comparison of maturity levels

Mitigation Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Patch applications	**An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.**	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services.
	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 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 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 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 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.
	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.	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 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.	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 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.	–
	–	–	**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 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 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.
	Online services that are no longer supported by vendors are removed.	Online services that are no longer supported by vendors are removed.	Online services 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.	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.
	–	–	**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.**
Patch operating systems	**An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.**	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.
	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 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 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 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 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 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 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 firmware.**
	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.	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 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.	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 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.	–

	–	–	**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 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 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 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 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 one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist.**
	–	–	**The latest release, or the previous release, of operating systems are used.**
	Operating systems that are no longer supported by vendors are replaced.	Operating systems that are no longer supported by vendors are replaced.	Operating systems that are no longer supported by vendors are replaced.
Multi-factor authentication	**Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.**	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.	Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data.
	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.	Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data.
	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.	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.	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.
	Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.	Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.	Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data.

Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.	Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.	Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data.
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.	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 privileged users of systems.**	Multi-factor authentication is used to authenticate privileged users of systems.
–	**Multi-factor authentication is used to authenticate unprivileged users of systems.**	Multi-factor authentication is used to authenticate unprivileged users of systems.
–	–	**Multi-factor authentication is used to authenticate users of data repositories.**
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.	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.	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.
–	**Multi-factor authentication used for authenticating users of online services is phishing-resistant.**	Multi-factor authentication used for authenticating users of online services is phishing-resistant.
–	**Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option.**	–
	–	**Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant.**
–	**Multi-factor authentication used for authenticating users of systems is phishing-resistant.**	Multi-factor authentication used for authenticating users of systems is phishing-resistant.
–	–	**Multi-factor authentication used for authenticating users of data repositories is phishing-resistant.**
–	**Successful and unsuccessful multi-factor authentication events are centrally logged.**	Successful and unsuccessful multi-factor authentication events are centrally logged.
–	**Event logs are protected from unauthorised modification and deletion.**	Event logs are protected from unauthorised modification and deletion.
–	**Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.**	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
–	–	**Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.**
–	–	**Event logs from workstations are analysed in a timely manner to detect cyber security events.**

	–	**Cyber security events are analysed in a timely manner to identify cyber security incidents.**	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	–	**Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.**	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
	–	**Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.**	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	–	**Following the identification of a cyber security incident, the cyber security incident response plan is enacted.**	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict administrative privileges	**Requests for privileged access to systems, applications and data repositories are validated when first requested.**	Requests for privileged access to systems, applications and data repositories are validated when first requested.	Requests for privileged access to systems, applications and data repositories are validated when first requested.
	–	**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.
	–	**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.
	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.
	–	–	**Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties.**
	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services.
	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.	Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties.
	–	–	**Secure Admin Workstations are used in the performance of administrative activities.**
	Privileged users use separate privileged and unprivileged operating environments.	Privileged users use separate privileged and unprivileged operating environments.	Privileged users use separate privileged and unprivileged operating environments.
	–	**Privileged operating environments are not virtualised within unprivileged operating environments.**	Privileged operating environments are not virtualised within unprivileged operating environments.
	Unprivileged user accounts cannot logon to privileged operating environments.	Unprivileged user accounts cannot logon to privileged operating environments.	Unprivileged user accounts cannot logon to privileged operating environments.

Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.
–	–	**Just-in-time administration is used for administering systems and applications.**
–	**Administrative activities are conducted through jump servers.**	Administrative activities are conducted through jump servers.
–	**Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.**	Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed.
–	–	**Memory integrity functionality is enabled.**
–	–	**Local Security Authority protection functionality is enabled.**
–	–	**Credential Guard functionality is enabled.**
–	–	**Remote Credential Guard functionality is enabled.**
–	**Privileged access events are centrally logged.**	Privileged access events are centrally logged.
–	**Privileged user account and security group management events are centrally logged.**	Privileged user account and security group management events are centrally logged.
–	**Event logs are protected from unauthorised modification and deletion.**	Event logs are protected from unauthorised modification and deletion.
–	**Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.**	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
–	–	**Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.**
–	–	**Event logs from workstations are analysed in a timely manner to detect cyber security events.**
–	**Cyber security events are analysed in a timely manner to identify cyber security incidents.**	Cyber security events are analysed in a timely manner to identify cyber security incidents.
–	**Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.**	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
–	**Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.**	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
–	**Following the identification of a cyber security incident, the cyber security incident response plan is enacted.**	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.

Application control	**Application control is implemented on workstations.**	Application control is implemented on workstations.	Application control is implemented on workstations.
	–	**Application control is implemented on internet-facing servers.**	Application control is implemented on internet-facing servers.
	–	–	**Application control is implemented on non-internet-facing servers.**
	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.	Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients.
	–	**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 is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients.
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.
	–	–	**Application control restricts the execution of drivers to an organisation-approved set.**
	–	**Microsoft's recommended application blocklist is implemented.**	Microsoft's recommended application blocklist is implemented.
	–	–	**Microsoft's vulnerable driver blocklist is implemented.**
	–	**Application control rulesets are validated on an annual or more frequent basis.**	Application control rulesets are validated on an annual or more frequent basis.
	–	**Allowed and blocked application control events are centrally logged.**	Allowed and blocked application control events are centrally logged.
	–	**Event logs are protected from unauthorised modification and deletion.**	Event logs are protected from unauthorised modification and deletion.
	–	**Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.**	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	–	–	**Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.**
	–	–	**Event logs from workstations are analysed in a timely manner to detect cyber security events.**
	–	**Cyber security events are analysed in a timely manner to identify cyber security incidents.**	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	–	**Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.**	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.
	–	**Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.**	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.

	–	**Following the identification of a cyber security incident, the cyber security incident response plan is enacted.**	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Restrict Microsoft Office macros	**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.	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.
	–	–	**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.**
	–	–	**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.**
	–	–	**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 signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View.**
	–	–	**Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.**
	Microsoft Office macros in files originating from the internet are blocked.	Microsoft Office macros in files originating from the internet are blocked.	Microsoft Office macros in files originating from the internet are blocked.
	Microsoft Office macro antivirus scanning is enabled.	Microsoft Office macro antivirus scanning is enabled.	Microsoft Office macro antivirus scanning is enabled.
	–	**Microsoft Office macros are blocked from making Win32 API calls.**	Microsoft Office macros are blocked from making Win32 API calls.
	Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macro security settings cannot be changed by users.	Microsoft Office macro security settings cannot be changed by users.
User application hardening	**Internet Explorer 11 is disabled or removed.**	Internet Explorer 11 is disabled or removed.	Internet Explorer 11 is disabled or removed.
	Web browsers do not process Java from the internet.	Web browsers do not process Java from the internet.	Web browsers do not process Java from the internet.
	Web browsers do not process web advertisements from the internet.	Web browsers do not process web advertisements from the internet.	Web browsers do not process web advertisements from the internet.
	–	**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 browser security settings cannot be changed by users.	Web browser security settings cannot be changed by users.	Web browser security settings cannot be changed by users.
	–	**Microsoft Office is blocked from creating child processes.**	Microsoft Office is blocked from creating child processes.
	–	**Microsoft Office is blocked from creating executable content.**	Microsoft Office is blocked from creating executable content.

	–	**Microsoft Office is blocked from injecting code into other processes.**	Microsoft Office is blocked from injecting code into other processes.
	–	**Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.**	Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.
	–	**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 suite security settings cannot be changed by users.**	Office productivity suite security settings cannot be changed by users.
	–	**PDF software is blocked from creating child processes.**	PDF software is blocked from creating child processes.
	–	**PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.**	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.
	–	**PDF software security settings cannot be changed by users.**	PDF software security settings cannot be changed by users.
	–	–	**.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.**
	–	–	**Windows PowerShell 2.0 is disabled or removed.**
	–	–	**PowerShell is configured to use Constrained Language Mode.**
	–	**PowerShell module logging, script block logging and transcription events are centrally logged.**	PowerShell module logging, script block logging and transcription events are centrally logged.
	–	**Command line process creation events are centrally logged.**	Command line process creation events are centrally logged.
	–	**Event logs are protected from unauthorised modification and deletion.**	Event logs are protected from unauthorised modification and deletion.
	–	**Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.**	Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events.
	–	–	**Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events.**
	–	–	**Event logs from workstations are analysed in a timely manner to detect cyber security events.**
	–	**Cyber security events are analysed in a timely manner to identify cyber security incidents.**	Cyber security events are analysed in a timely manner to identify cyber security incidents.
	–	**Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.**	Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered.

	–	**Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.**	Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.
	–	**Following the identification of a cyber security incident, the cyber security incident response plan is enacted.**	Following the identification of a cyber security incident, the cyber security incident response plan is enacted.
Regular backups	**Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.**	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements.
	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.	Backups of data, applications and settings are synchronised to enable restoration to a common point in time.
	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.	Backups of data, applications and settings are retained in a secure and resilient manner.
	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.	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
	Unprivileged user accounts cannot access backups belonging to other user accounts.	Unprivileged user accounts cannot access backups belonging to other user accounts.	Unprivileged user accounts cannot access backups belonging to other user accounts.
	–	–	**Unprivileged user accounts cannot access their own backups.**
	–	**Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.**	Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts.
	–	–	**Privileged user accounts (excluding backup administrator accounts) cannot access their own backups.**
	Unprivileged user accounts are prevented from modifying and deleting backups.	Unprivileged user accounts are prevented from modifying and deleting backups.	Unprivileged user accounts are prevented from modifying and deleting backups.
	–	**Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.**	Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.
	–	–	**Backup administrator accounts are prevented from modifying and deleting backups during their retention period.**

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2023.

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.



The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)



Australian Government

Australian Signals Directorate