Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Essential Eight Maturity Model

First published: June 2017
Last updated: November 2022

Introduction

The Australian Cyber Security Centre (ACSC) 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 Microsoft Windows-based internet-connected networks. While the principles behind the Essential Eight may be applied to cloud services and enterprise mobility, or other operating systems, it was not primarily designed for such purposes and alternative mitigation strategies may be more appropriate to mitigate unique cyber threats to these environments. In such cases, organisations should consider alternative guidance provided by the ACSC.

The *Essential Eight Maturity Model*, first published in June 2017 and updated regularly, supports the implementation of the Essential Eight. It is based on the ACSC'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 security 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 security 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 security 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 adversary tradecraft (i.e. tools, tactics, techniques and procedures) and targeting, which are discussed in more detail below. Depending on an adversary's overall capability, they may exhibit different levels of tradecraft for different operations against different targets. For example, an adversary 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 adversaries, they are aiming to mitigate.

Organisations need to consider that the likelihood of being targeted is influenced by their desirability to adversaries, 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 adversaries 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 adversaries who are content to simply leverage commodity tradecraft that is widely available in order to gain access to, and likely control of, systems. For example, adversaries opportunistically using a publicly-available exploit for a security vulnerability in an internet-facing service which had not been patched, or authenticating to an internet-facing service using credentials that were stolen, reused, brute forced or guessed.

Generally, adversaries 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. Adversaries will employ common social engineering techniques to trick users into weakening the security of a system and launch malicious applications, for example via Microsoft Office macros. If the account that an adversary compromises has special privileges they will seek to exploit it. Depending on their intent, adversaries may also destroy data (including backups).

Maturity Level Two

The focus of this maturity level is adversaries operating with a modest step-up in capability from the previous maturity level. These adversaries are willing to invest more time in a target and, perhaps more importantly, in the effectiveness of their tools. For example, these adversaries will likely employ well-known tradecraft in order to better attempt to bypass security 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, adversaries 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. Adversaries 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, for example via Microsoft Office macros. If the account that an adversary compromises has special privileges they will seek to exploit it, otherwise they will seek accounts with special privileges. Depending on their intent, adversaries may also destroy all data (including backups) accessible to an account with special privileges.

Maturity Level Three

The focus of this maturity level is adversaries who are more adaptive and much less reliant on public tools and techniques. These adversaries 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. Adversaries 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. Adversaries make swift use of exploits when they become publicly available as well as other tradecraft that can improve their chance of success.

Generally, adversaries 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 security 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 security 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, adversaries will seek to gain privileged credentials or password hashes, pivot to other parts of a network, and cover their tracks. Depending on their intent, adversaries 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 about 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 additional mitigation strategies is available in the *Strategies to Mitigate Cyber Security Incidents – Mitigation Details* publication.
- Further Information on implementing application control is available in the *Implementing Application Control* publication.
- Further Information on patching is available in the *Assessing Security Vulnerabilities and Applying Patches* publication.
- Further Information on controlling Microsoft Office macros is available in the *Microsoft Office Macro Security* publication.
- Further Information on controlling privileged accounts is available in the *Restricting Administrator Privileges* publication.
- Further Information on implementing multi-factor authentication is available in the *Implementing Multi-Factor Authentication* 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
Application control	The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.
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 security vulnerabilities in internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. Internet-facing services, 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.
Configure Microsoft Office macro settings	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	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 does not process content from the internet. Web browser security settings cannot be changed by users.

Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested. Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.
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 security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and 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 by an organisation's users if they authenticate to their organisation’s internet-facing services. Multi-factor authentication is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation’s users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation’s internet-facing services.
Regular backups	Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements.

Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time.

Backups of important data, software and configuration settings are retained in a secure and resilient manner.

Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises.

Unprivileged accounts cannot access backups belonging to other accounts.

Unprivileged accounts are prevented from modifying and deleting backups.

Appendix B: Maturity Level Two

Mitigation Strategy	Description
Application control	Application control is implemented on workstations and internet-facing servers. Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set. Allowed and blocked execution events on workstations and internet-facing servers are logged.
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 security vulnerabilities in internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or updates for security 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 security vulnerabilities in other applications. Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security 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 vendor mitigations for security vulnerabilities in other applications are applied within one month of release. Internet-facing services, 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.
Configure Microsoft Office macro settings	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.

	Allowed and blocked Microsoft Office macro execution events are logged.
User application hardening	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 does not process content from the internet. 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 OLE packages. PDF software is blocked from creating child processes. ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented. Web browser, Microsoft Office and PDF software security settings cannot be changed by users. Blocked PowerShell script execution events are logged.
Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested. Privileged access to systems and applications is automatically disabled after 12 months unless revalidated. Privileged access to systems and applications is automatically disabled after 45 days of inactivity. Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Privileged operating environments are not virtualised within unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. Administrative activities are conducted through jump servers. Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed. Privileged access events are logged. Privileged account and group management events are logged.
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 security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release. Operating systems that are no longer supported by vendors are replaced.
Multi-factor authentication	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services. Multi-factor authentication is used to authenticate privileged 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. Successful and unsuccessful multi-factor authentication events are logged.
Regular backups	Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time. Backups of important data, software and configuration settings are retained in a secure and resilient manner. Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises. Unprivileged accounts cannot access backups belonging to other accounts. Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.

Unprivileged accounts are prevented from modifying and deleting backups.

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

Appendix C: Maturity Level Three

Mitigation Strategy	Description
Application control	Application control is implemented on workstations and servers. Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets and drivers to an organisation-approved set. Microsoft's 'recommended block rules' are implemented. Microsoft's 'recommended driver block rules' are implemented. Application control rulesets are validated on an annual or more frequent basis. Allowed and blocked execution events on workstations and servers are centrally logged. Event logs are protected from unauthorised modification and deletion. Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.
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 security vulnerabilities in internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or updates for security 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 security vulnerabilities in other applications. Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month of release. Applications that are no longer supported by vendors are removed.

Configure Microsoft Office macro settings	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. Only privileged users responsible for validating 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'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. Allowed and blocked Microsoft Office macro execution events are centrally logged. Event logs are protected from unauthorised modification and deletion. Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.
User application hardening	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 is disabled or removed. 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 OLE packages. PDF software is blocked from creating child processes. ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented. Web browser, Microsoft Office and 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. Blocked PowerShell script execution events are centrally logged. Event logs are protected from unauthorised modification and deletion.

	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.
Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested. Privileged access to systems and applications is automatically disabled after 12 months unless revalidated. Privileged access to systems and applications is automatically disabled after 45 days of inactivity. Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties. Privileged accounts are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Privileged operating environments are not virtualised within unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged 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 local administrator accounts and service accounts are long, unique, unpredictable and managed. Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled. Privileged access events are centrally logged. Privileged account and group management events are centrally logged. Event logs are protected from unauthorised modification and deletion. Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.
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 security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices.

	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release, or within 48 hours if an exploit exists. 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 by an organisation's users if they authenticate to their organisation's internet-facing services. Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services. Multi-factor authentication is used to authenticate privileged users of systems. Multi-factor authentication is used to authenticate users accessing important data repositories. Multi-factor authentication is verifier impersonation resistant and uses either: something users have and something users know, or something users have that is unlocked by something users know or are. Successful and unsuccessful multi-factor authentication events are centrally logged. Event logs are protected from unauthorised modification and deletion. Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.
Regular backups	Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time. Backups of important data, software and configuration settings are retained in a secure and resilient manner. Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises.

Unprivileged accounts cannot access backups belonging to other accounts, nor their own accounts.

Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts, nor their own accounts.

Unprivileged accounts are prevented from modifying and deleting backups.

Privileged accounts (including backup administrator accounts) are prevented from modifying and deleting backups during their retention period.

Appendix D: Comparison of maturity levels

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Application control	The execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets is prevented on workstations from within standard user profiles and temporary folders used by the operating system, web browsers and email clients.	**Application control is implemented on workstations and internet-facing servers.** **Application control restricts** the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets **to an organisation-approved set**. **Allowed and blocked execution events on workstations and internet-facing servers are logged.**	Application control is implemented on workstations and **servers**. Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications, control panel applets **and drivers** to an organisation-approved set. **Microsoft's 'recommended block rules' are implemented.** **Microsoft's 'recommended driver block rules' are implemented.** **Application control rulesets are validated on an annual or more frequent basis.** Allowed and blocked execution events on workstations and **servers** are **centrally** logged. **Event logs are protected from unauthorised modification and deletion.** **Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.**
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 security vulnerabilities in internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. Internet-facing services, 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.	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 security vulnerabilities in internet-facing services. A vulnerability scanner is used at least **weekly** to identify missing patches or updates for security 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 security vulnerabilities in other applications.** Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security 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 vendor mitigations for security vulnerabilities in other applications are applied within one month of release.** Internet-facing services, 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.	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 security vulnerabilities in internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or updates for security 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 security vulnerabilities in other applications. Patches, updates or vendor mitigations for security vulnerabilities in internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release, **or within 48 hours if an exploit exists**. Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month of release. **Applications** that are no longer supported by vendors are removed.

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Configure Microsoft Office macro settings	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.	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. **Allowed and blocked Microsoft Office macro execution events are logged.**	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.** **Only privileged users responsible for validating 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'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. Allowed and blocked Microsoft Office macro execution events are **centrally** logged. **Event logs are protected from unauthorised modification and deletion.** **Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.**
User application hardening	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 does not process content from the internet. Web browser security settings cannot be changed by users.	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 does not process content from the internet. **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 OLE packages.** **PDF software is blocked from creating child processes.** **ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.** Web browser, **Microsoft Office and PDF software** security settings cannot be changed by users. **Blocked PowerShell script execution events are logged.**	Web browsers do not process Java from the internet. Web browsers do not process web advertisements from the internet. Internet Explorer 11 **is disabled or removed**. 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 OLE packages. PDF software is blocked from creating child processes. ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented. Web browser, Microsoft Office and 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.** Blocked PowerShell script execution events are **centrally** logged. **Event logs are protected from unauthorised modification and deletion.** **Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.**

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested. Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	Requests for privileged access to systems and applications are validated when first requested. **Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.** **Privileged access to systems and applications is automatically disabled after 45 days of inactivity.** Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. **Privileged operating environments are not virtualised within unprivileged operating environments.** Unprivileged accounts cannot logon to privileged operating environments. Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. **Administrative activities are conducted through jump servers.** **Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed.** **Privileged access events are logged.** **Privileged account and group management events are logged.**	Requests for privileged access to systems and applications are validated when first requested. Privileged access to systems and applications is automatically disabled after 12 months unless revalidated. Privileged access to systems and applications is automatically disabled after 45 days of inactivity. **Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.** **Privileged accounts** are prevented from accessing the internet, email and web services. Privileged users use separate privileged and unprivileged operating environments. Privileged operating environments are not virtualised within unprivileged operating environments. Unprivileged accounts cannot logon to privileged operating environments. Privileged 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 local administrator accounts and service accounts are long, unique, unpredictable and managed. **Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.** Privileged access events are **centrally** logged. Privileged account and group management events are **centrally** logged. **Event logs are protected from unauthorised modification and deletion.** **Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.**

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
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 security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within one month of release. Operating systems that are no longer supported by vendors are replaced.	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 security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least **weekly** to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within **two weeks** of release. Operating systems that are no longer supported by vendors are replaced.	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 security vulnerabilities in operating systems of internet-facing services. A vulnerability scanner is used at least weekly to identify missing patches or updates for security vulnerabilities in operating systems of workstations, servers and network devices. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of internet-facing services are applied within two weeks of release, or within 48 hours if an exploit exists. Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release, **or within 48 hours if an exploit exists**. **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 by an organisation's users if they authenticate to their organisation's internet-facing services. Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services.	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services. **Multi-factor authentication is used to authenticate privileged 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.** **Successful and unsuccessful multi-factor authentication events are logged.**	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services. Multi-factor authentication is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's sensitive data. Multi-factor authentication (where available) is used by an organisation's users if they authenticate to third-party internet-facing services that process, store or communicate their organisation's non-sensitive data. Multi-factor authentication is enabled by default for non-organisational users (but users can choose to opt out) if they authenticate to an organisation's internet-facing services. Multi-factor authentication is used to authenticate privileged users of systems. **Multi-factor authentication is used to authenticate users accessing important data repositories.** Multi-factor authentication **is verifier impersonation resistant and** uses either: something users have and something users know, or something users have that is unlocked by something users know or are. Successful and unsuccessful multi-factor authentication events are **centrally** logged. **Event logs are protected from unauthorised modification and deletion.** **Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.**

Strategy	Maturity Level One	Maturity Level Two	Maturity Level Three
Regular backups	Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time. Backups of important data, software and configuration settings are retained in a secure and resilient manner. Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises. Unprivileged accounts cannot access backups belonging to other accounts. Unprivileged accounts are prevented from modifying and deleting backups.	Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time. Backups of important data, software and configuration settings are retained in a secure and resilient manner. Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises. Unprivileged accounts cannot access backups belonging to other accounts. **Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.** Unprivileged accounts are prevented from modifying and deleting backups. **Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.**	Backups of important data, software and configuration settings are performed and retained with a frequency and retention timeframe in accordance with business continuity requirements. Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time. Backups of important data, software and configuration settings are retained in a secure and resilient manner. Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises. Unprivileged accounts cannot access backups belonging to other accounts**, nor their own accounts**. Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts**, nor their own accounts**. Unprivileged accounts are prevented from modifying and deleting backups. Privileged accounts (**including** backup administrator accounts) are prevented from modifying and deleting backups **during their retention period**.