Australian Government
Australian Signals Directorate

Essential Eight Maturity Model FAQ

First published: July 2021
Last updated: September 2023

Introduction

This publication was developed to answer frequently asked questions on the *Essential Eight Maturity Model* (E8MM).

Frequently asked questions

General questions

What is the Essential Eight?

- While no set of mitigation strategies are guaranteed to protect against all cyber threats, organisations are recommended to implement eight essential mitigation strategies from the *Strategies to Mitigate Cyber Security Incidents* as a baseline. This baseline, known as the Essential Eight, makes it much harder for malicious actors to compromise systems.
- The mitigation strategies that constitute the Essential Eight are: application control, patch applications, configure Microsoft Office macro settings, user application hardening, restrict administrative privileges, patch operating systems, multi-factor authentication and regular backups.

Why should I implement the Essential Eight?

- Implementing the Essential Eight proactively can be more cost-effective in terms of time, money and effort than having to respond to a large-scale cyber security incident.

What is the *Essential Eight Maturity Model*?

- The E8MM is designed to assist organisations to implement the Essential Eight in a graduated manner based upon different levels of malicious actors' tradecraft (i.e. tools, tactics, techniques and procedures) and targeting.
- The different maturity levels can also be used to provide a high-level indication of an organisation's cyber security maturity.

Why update the *Essential Eight Maturity Model*?

- The Australian Signals Directorate (ASD) is committed to providing cyber security advice that is contemporary, fit for purpose and practical. This includes regular updates to the E8MM.
- Malicious actors continually evolve their tradecraft to defeat preventative measures that organisations put in place.

- ASD continually learns of advances in malicious actors' tradecraft through its cyber threat intelligence and cyber security incident response functions.
- ASD also learns of how our cyber security advice is implemented within organisations as part of Essential Eight implementation assessments and uplift activities.
- Updates to the E8MM follow a thorough review by ASD, which includes consultation with government and industry partners.

Which version of the *Essential Eight Maturity Model* should be used?

- Organisations are strongly encouraged to use the latest version of the E8MM to protect themselves against contemporary tradecraft used by malicious actors. Note, legacy versions of the E8MM will often no longer be fit for purpose due to the continual evolution of tradecraft used by malicious actors.

How do the *Essential Eight Maturity Model* and *Information Security Manual* relate to each other?

- The applicability of controls within the *Information Security Manual* (ISM) is based on the classification of data that a system will store, process or communicate whereas the E8MM is based on prioritising the implementation of controls to mitigate different levels of malicious actors' tradecraft and targeting.
- A mapping between the E8MM and ISM is provided within the *Essential Eight Maturity Model and ISM Mapping* publication.
- The ISM also provides OSCAL baselines for the E8MM which can be used by organisations to track their implementation of the E8MM within their governance, reporting and compliance tools.
- Organisations should consider their E8MM and ISM requirements independently. For example, an organisation contractually required to implement Maturity Level Two from the E8MM should not assume that controls within the ISM that are mapped to Maturity Level Three are out of scope when building and deploying a system. For non-corporate Commonwealth entities subject to the Department of Home Affairs' *Protective Security Policy Framework*, this means that while Maturity Level Two is considered a mandatory baseline, controls mapped to Maturity Level Three within the ISM are still applicable for their systems, however, their implementation may be risk managed.

Is there any training available on the *Essential Eight Maturity Model*?

- ASD has developed an Essential Eight assessment course and partnered with TAFEcyber for the delivery of the course to cyber security professionals across Australia.
- The Essential Eight assessment course is a face-to-face three-day course that uses a blend of specialist expertise, knowledge and hands-on technical training. Further information on the Essential Eight Assessment Course is available from TAFEcyber.

Essential Eight Maturity Model update (November 2022)

What were the updates?

- Organisations are recommended to use an automated method of asset discovery at least fortnightly to detect what assets reside on their network (to assist with follow-on vulnerability scanning activities).
- Organisations are recommended to ensure their vulnerability scanners are using an up-to-date vulnerability database before conducting vulnerability scanning activities.
- Minor grammar amendments were made throughout for increased clarity (these changes have not changed the intent of existing requirements).

Implementation questions – General

Is the *Essential Eight Maturity Model* applicable to all systems?

- 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.

Are legacy systems out of scope?

- It is often difficult to implement the Essential Eight, either in part or in full, on legacy systems. In such cases, ASD strongly encourages organisations to upgrade their legacy systems as a priority so that the Essential Eight can be implemented in full. While a system is in the process of being upgraded, organisations should implement compensating controls where possible to do so.

What maturity level should I target?

- Generally, Maturity Level One may be suitable for small to medium enterprises, Maturity Level Two may be suitable for large enterprises, and Maturity Level Three may be suitable for critical infrastructure providers and other organisations that operate in high threat environments.
- When implementing Essential Eight requirements, 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.
- For organisations with a target maturity level above Maturity Level One, they may choose to implement individual requirements of a higher maturity level if it is more efficient and cost-effective to do so in the long run. For example, rather than implementing physical one-time password tokens to meet Maturity Level Two requirements, then later replacing them with phishing-resistant smart cards or security keys to meet Maturity Level Three requirements, organisations may choose to implement smart cards or security keys when implementing Maturity Level Two.
- Organisations should not be penalised for implementing more robust security measures than specified for the given maturity level they are being assessed against.

Can I jump straight to implementing my target maturity level?

- Organisations should progressively implement, and assess their implementation of, each maturity level until their target maturity level is achieved. Using such an approach provides organisations the opportunity to validate the correctness and robustness of their implementation of a particular maturity level before moving onto the next maturity level.
- Using a staged approach also allows organisations to:
  - assess the effectiveness of any new controls within their environment
  - monitor for any unanticipated consequences and identify any edge cases
  - address any issues identified following an assessment of their implementation
  - identify any impacted business processes, including unanticipated consequences
  - allow employees time to adjust to changes within their environment and work flows.

Can I implement compensating controls instead of specific Essential Eight requirements?

- Yes. However, system owners will need to demonstrate that their compensating controls provide an equivalent level of protection to the specific Essential Eight requirements they are compensating for. This will assist in ensuring that an equivalent level of overall protection against a specified level of malicious actors' tradecraft and targeting can be achieved and maintained.

- In cases where compensating controls are implemented, a mitigation strategy will be considered to have been fully implemented when all requirements that form that mitigation strategy have been assessed as either implemented or implemented using suitable compensating controls. However, if compensating controls are assessed as not suitable, the mitigation strategy will be assessed as either the next lowest maturity level it qualifies for or Maturity Level Zero.
- Note, system owners that seek to use risk acceptance without compensating controls, or risk transference (e.g. by sourcing cyber insurance), as justification for not implementing an entire mitigation strategy, such as application control or multi-factor authentication, will be considered to have not protected themselves against a specific class of cyber threat and will subsequently be assessed as Maturity Level Zero for both that mitigation strategy and their overall Essential Eight implementation.

What is a workstation?

- A workstation is any device that uses a desktop operating system, such as Microsoft Windows or a Linux distribution. This includes traditional desktop PCs, laptops and some tablets.

What is an internet-facing server?

- An internet-facing server is any server that is directly accessible over the internet.

What is an internet-facing service?

- An internet-facing service (also known as an online service) is any service that is directly accessible over the internet, including those sitting behind a perimeter firewall. For example, a web portal, a cloud service or a network device (such as a firewall or VPN concentrator).
- An example of an internet-facing service that processes, stores or communicates an organisation's sensitive data is any cloud service that has been authorised for use with OFFICIAL: Sensitive or PROTECTED data (such as GovTeams) or any other sensitive business data.
- Examples of internet-facing services that process, store or communicate an organisation's non-sensitive data can include web hosting services (such as GovCMS) or social media platforms (such as Facebook, Instagram, LinkedIn, YouTube and X).

Does ASD provide a list of approved products for implementing the Essential Eight?

- No. Organisations should determine the suitability of particular products based on their own requirements.

Does ASD provide any tools to assist with assessing implementations of the Essential Eight?

- Yes. ASD provides two tools as part of a 'cyber toolbox' to assist organisations with assessing implementations of the Essential Eight. These tools are the Essential Eight Maturity Verification Tool (E8MVT) and the Application Control Verification Tool (ACVT).
- Both E8MVT and ACVT are available to download via ASD's Partner Portal.

Do I require a Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) or Extended Detection and Response (XDR) solution to capture, protect and monitor event logs?

- The *Strategies to Mitigate Cyber Security Incidents* publication recommends the use of SIEM and EDR software to centrally log and analyse system behaviour to detect compromises, while also facilitating cyber security incident response activities.
- MITRE's research illustrates how various EDR vendors can detect and respond to compromises of systems by malicious actors.
- Recent industry advances have introduced the concept of XDR which combines SIEM and EDR functionality while adding more advanced log analysis capabilities. This often integrates cloud-based analysis of host-based sensor telemetry to link disparate alerts in order to detect compromises of systems.

Can I filter out events from event logs that are known to be legitimate in order to simplify event log analysis and reduce storage requirements?

- Yes. Organisations that are comfortable that certain events have a high probability of being legitimate may choose to filter them out of event logs in order to simplify event log analysis and reduce storage requirements.

Do I need to perform events log analysis in real time or near real time?

- Organisations should analyse event logs for signs of compromise in a timeframe that is reasonably practicable given the resources they have available to them.

Implementation questions – Application control

Do I need to use an application control solution for Maturity Level One?

- No. While an application control solution may be used at this maturity level, it may also be achieved using file system access permissions.

What file types do I need to control with my application control solution?

- The following in a non-exhaustive list of common file types that can be controlled by application control solutions:
  - **executables:** .exe and .com files
  - **software libraries:** .dll and .ocx files
  - **scripts:** .ps1, .bat, .cmd, .vbs and .js files
  - **installers:** .msi, .msp and .mst files
  - **compiled HTML:** .chm files
  - **HTML applications:** .hta files
  - **control panel applets:** .cpl files.

Where can I find Microsoft's 'recommended block rules'?

- Information on Microsoft's 'recommended block rules' is available from Microsoft.

Where can I find Microsoft's 'recommended driver block rules'?

- Information on Microsoft's 'recommended driver block rules', also known as the vulnerable driver blocklist, is available from Microsoft.

Can Microsoft's 'recommended driver block rules' be implemented using core isolation's memory integrity functionality?

- Yes. Enabling core isolation's memory integrity functionality will automatically enforce Microsoft's 'recommended driver block rules', also known as the vulnerable driver blocklist. This approach is preferred by Microsoft over the use of Windows Defender Application Control (WDAC) to block vulnerable or malicious drivers.
- Microsoft reviews their vulnerable driver blocklist every 6-12 months and updates it automatically for organisations that have implemented core isolation's memory integrity functionality. In contrast, organisations using WDAC will need to manually update their application control rulesets when Microsoft releases updated 'recommended driver block rules'.
- From Windows 11 version 22H2 onwards, the vulnerable driver blocklist is enabled by default.

Implementation questions – Patch applications

My vulnerability scanning tool offers the ability to automatically detect assets on a network, can I use it as an asset discovery tool?

- Yes. Some vulnerability scanning tools offer automatic asset discovery functionality that is equivalent to other tools developed for that sole purpose.

Can I perform automated asset discovery more frequently than fortnightly?

- Yes. While automated asset discovery should be performed at least fortnightly, system owners may elect to align the frequency of asset discovery scans to more frequent timeframes used for vulnerability scans (such as daily or weekly) in order to perform both activities at the same time for optimal effect.

How can I find out if a vulnerability has a working exploit?

- Vendors, ASD, news outlets and security researchers often cover exploitable vulnerabilities.
- The United State's Cybersecurity & Infrastructure Security Agency also maintains a *Known Exploited Vulnerabilities Catalog*.

One of my vendors doesn't rate the criticality of vulnerabilities, what should I do?

- ASD, news outlets and security researchers often cover critical vulnerabilities.
- Organisations may also consider the type of vulnerability, including factors such as its Common Vulnerability Scoring System score (if available), to determine if it would have likely represented a critical vulnerability.

Do I have 48 hours to patch from when working exploits are announced or when exploitation starts occurring?

- The requirement to patch within 48 hours when a working exploit exists relates to the announcement of a working exploit or that exploitation is already occurring, whichever occurs first.

I'm unable to perform rapid scanning and patching of internet-facing services, what can I do?

- ASD encourages all organisations to consider moving their internet-facing services to mature and trustworthy cloud service providers. Depending on the type of cloud service used, this can result in significant security benefits such as the rapid identification and patching of vulnerabilities.

How can I remove Adobe Flash Player?

- Information on removing Adobe Flash Player, if installed automatically by Microsoft Windows, is available from Microsoft.
- Information on removing Adobe Flash Player, if installed manually, is available from Adobe.

Implementation questions – Configure Microsoft Office macro settings

Can I use Application Guard for Office to execute macros in a sandboxed environment?

- Unfortunately, no. Application Guard for Office disables the execution of macros in Microsoft Office documents.

Can I use Application Guard for Office to block the execution of macros?

- Unfortunately, Application Guard for Office is limited in its ability to provide a comprehensive solution to blocking the execution of macros within organisations. Specifically, Microsoft Office documents will only be opened in Application Guard for Office when identified as originating from an untrusted source, such as the internet.

- As Application Guard for Office cannot be configured to always activate when opening Microsoft Office documents, this will not prevent the execution of macros that were developed internally to organisations (e.g. by malicious insiders) or from Microsoft Office documents that have had the Mark of the Web removed from them (e.g. due to users being convinced by malicious actors to do so as part of social engineering efforts).

Implementation questions – User application hardening

Does this mitigation strategy apply to servers?

- Yes. Although some user applications, such as Microsoft Office and PDF software, may not be present on servers.

Does preventing web browsers from processing Java from the internet include JavaScript?

- No. The requirement to prevent web browsers from processing Java from the internet does not include JavaScript.

Where can I find information on using attack surface reduction rules?

- Information on using attack surface reduction rules is available from Microsoft.
- Information on using attack surface reduction rules is also available in the *Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016* publication.

Where can I find information on preventing the activation of OLE packages?

- Information on preventing the activation of OLE packages is available in the *Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016* publication.

Where can I find ASD hardening guidance?

- Further system hardening guidance is available from ASD.

When ASD and vendor hardening guidance differ, which do I follow?

- In situations where ASD and vendor hardening guidance differs, each difference should be assessed on a case-by-case basis; however, preference should be given to implementing the most restrictive requirements.

Implementation questions – Restrict administrative privileges

What are unprivileged operating environments?

- Unprivileged operating environments are those used for activities that do not require privileged access, such as reading emails and browsing the web.

What are privileged operating environments?

- Privileged operating environments are those used for activities that require a degree of privileged access, such as system administration activities.

What are unprivileged accounts?

- Unprivileged accounts include unprivileged user accounts and unprivileged service accounts.

What are privileged accounts?

- Privileged accounts include privileged user accounts and privileged service accounts.

What are privileged user accounts?

- Privileged user accounts generally have the capability to modify system configurations, account privileges, event logs and security configurations for applications. This also applies to users who may only have limited privileges but still have the ability to bypass some of a system's controls.

Where can I find information on hardening privileged operating environments?

- Microsoft provides a number of resources on securing privileged access, including the use of Privileged Access Workstations (PAWs).

Where can I find information on privileged access management?

- Microsoft provides an overview of privileged access management (PAM), including the concepts of just enough administration (JEA) and just-in-time (JIT) access.

What constitutes long credentials for local administrator accounts and service accounts?

- Long credentials are a minimum of 30 characters.

Where can I find information on Credential Guard and Remote Credential Guard?

- Information on Credential Guard functionality and Remote Credential Guard functionality is available from Microsoft.

Implementation questions – Patch operating systems

My vulnerability scanning tool offers the ability to automatically detect assets on a network, can I use it as an asset discovery tool?

- Yes. Some vulnerability scanning tools offer automatic asset discovery functionality that is equivalent to other tools developed for that sole purpose.

Can I perform automated asset discovery more frequently than fortnightly?

- Yes. While automated asset discovery should be performed at least fortnightly, system owners may elect to align the frequency of asset discovery scans to more frequent timeframes used for vulnerability scans (such as daily or weekly) in order to perform both activities at the same time for optimal effect.

How can I find out if a vulnerability has a working exploit?

- Vendors, ASD, news outlets and security researchers often cover exploitable vulnerabilities.
- The United State's Cybersecurity & Infrastructure Security Agency also maintains a *Known Exploited Vulnerabilities Catalog*.

One of my vendors doesn't rate the criticality of vulnerabilities, what should I do?

- ASD, news outlets and security researchers often cover critical vulnerabilities.
- Organisations may also consider the type of vulnerability, including factors such as its Common Vulnerability Scoring System score (if available), to determine if it would have likely represented a critical vulnerability.

Do I have 48 hours to patch from when working exploits are announced or when exploitation starts occurring?

- The requirement to patch within 48 hours when a working exploit exists relates to the announcement of a working exploit or that exploitation is already occurring, whichever occurs first.

What constitutes the previous release of an operating system?

- This depends on the servicing branch being used for the operating system (i.e. Semi-Annual Channel or Long-Term Servicing Channel).
- Information on Microsoft Windows 10, Microsoft Windows 11 and Microsoft Windows Server operating system releases is available from Microsoft.

Implementation questions – Multi-factor authentication

Following multi-factor authentication to a system or service, can I use a single factor for re-authentication?

- No. Multi-factor authentication is required for both authentication and re-authentication activities.

Can I use biometrics as a primary authentication factor?

- For Maturity Level One, biometrics can be used as a primary authenticator factor.
- For Maturity Level Two and higher, biometrics can only be used as a secondary authenticator factor to unlock something you have.

Can I use Trusted Signals as a primary authentication factor?

- For Maturity Level One, Trusted Signals can be used as a primary authentication factor.
- For Maturity Level Two and higher, Trusted Signals cannot be used as a primary authentication factor. However, organisations may use Trusted Signals in addition to two other suitable authentication factors for added security.
- Information on Trusted Signals is available from Microsoft.

Can I use Windows Hello for Business for multi-factor authentication?

- Yes. Windows Hello for Business uses biometrics (something users are) or a PIN (something users know) to unlock a key or certificate that is tied to a device's Trusted Platform Module (something users have).
- Information on the use of Windows Hello for Business is available from Microsoft.

What authentication types can be used for something users know?

- The following authentication types can be used for something users know: memorised secrets.
- The use of knowledge-based authentication techniques (i.e. security questions) is not recognised as a valid form of memorised secret.
- Further information can be found in Section 5.1.1 of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*.

What authentication types can be used for something users have?

- The following authentication types can be used for something users have: look-up secrets, out-of-band devices, single-factor OTP devices, single-factor cryptographic software and single-factor cryptographic devices.
- Further information can be found in Section 5.1.2, Section 5.1.3, Section 5.1.4, Section 5.1.6 and Section 5.1.7 respectively of NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*.

What authentication types can be used for something users have that is unlocked by something users know or are?

- The following authentication types can be used for something users have that is unlocked by something users know or are: multi-factor OTP devices, multi-factor cryptographic software and multi-factor cryptographic devices.

- Further information can be found in Section 5.1.5, Section 5.1.8 and Section 5.1.9 respectively of NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*.

Where can I find information on certified multi-factor authentication solutions?

- The FIDO Alliance certifies multi-factor authentication solutions against its UAF, U2F and FIDO2 standards.
- Organisations are encouraged to use multi-factor authentication solutions that have been certified against the FIDO2 standard (preferably Level 2 over Level 1).

Should I implement phishing-resistant multi-factor authentication for Maturity Level Two and below?

- While Maturity Level Two and below does not currently specify phishing-resistant multi-factor authentication at this time, ASD strongly encourages its use where supported.

Implementation questions – Regular backups

Can I delete backup contents to satisfy privacy or legal requirements?

- Yes. Depending on the maturity level, this may be done with either a privileged account, a backup administrator account or a break glass account.
- For Maturity Level Three, break glass accounts should only be used for this purpose.

Contact details

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