Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Essential Eight to ISM Mapping

JUNE 2020

Introduction

The ***Strategies to Mitigate Cyber Security Incidents*** is a prioritised list of mitigation strategies to assist organisations in protecting their systems against a range of adversaries. While no single mitigation strategy is guaranteed to prevent cyber security incidents, organisations are recommended to implement eight essential mitigation strategies as a baseline. This baseline, known as the Essential Eight, makes it much harder for adversaries to compromise systems.

This document provides a mapping between Maturity Level 3 of the ***Essential Eight Maturity Model*** and the security controls within the ***Australian Government Information Security Manual*** (ISM). This mapping represents the minimum security controls organisations must implement to meet the intent of the Essential Eight.

While this document outlines the minimum security controls to meet the intent of the Essential Eight, additional supporting security controls exist within the ISM. These supporting security controls should also be considered when implementing the Essential Eight.

Mitigation strategies to prevent malware delivery and execution

Application control

Application control *to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.*

Security Control: 0843; Revision: 8; Updated: Apr-20; Applicability: O, P, S, TS
Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set.

Security Control: 1490; Revision: 2; Updated: Apr-20; Applicability: O, P, S, TS
Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.

Security Control: 1544; Revision: 1; Updated: Apr-20; Applicability: O, P, S, TS
Microsoft's latest recommended block rules are implemented to prevent application control bypasses.

Patch applications

Patch applications *e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.*

Security Control: 1144; Revision: 9; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in applications and drivers assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.

Security Control: 1497; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
An automated mechanism is used to confirm and record that deployed application and driver patches or updates have been installed, applied successfully and remain in place.

Security Control: 0304; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Applications that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Configure Microsoft Office macro settings

Configure Microsoft Office macro settings *to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.*

Security Control: 1487; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros.

Security Control: 1488; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Microsoft Office macros in documents originating from the internet are blocked.

Security Control: 1489; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Microsoft Office macro security settings cannot be changed by users.

User application hardening

User application hardening. *Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.*

Security Control: 1484; Revision: 1; Updated: Jan-19; Applicability: O, P, S, TS
Web browsers are configured to block or disable support for Flash content.

Security Control: 1485; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Web browsers are configured to block web advertisements.

Security Control: 1486; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Web browsers are configured to block Java from the internet.

Security Control: 1541; Revision: 0; Updated: Jan-19; Applicability: O, P, S, TS
Microsoft Office is configured to disable support for Flash content.

Security Control: 1542; Revision: 0; Updated: Jan-19; Applicability: O, P, S, TS
Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

Mitigation strategies to limit the extent of cyber security incidents

Restrict administrative privileges

Restrict administrative privileges *to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.*

Security Control: 1507; Revision: 1; Updated: Sep-19; Applicability: O, P, S, TS
Privileged access to systems, applications and data repositories is validated when first requested and revalidated on an annual or more frequent basis.

Security Control: 1508; Revision: 1; Updated: Sep-19; Applicability: O, P, S, TS
Privileged access to systems, applications and data repositories is limited to that required for personnel to undertake their duties.

Security Control: 1175; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Technical security controls are used to prevent privileged users from reading emails, browsing the web and obtaining files via online services.

Patch operating systems

Patch operating systems. *Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.*

Security Control: 1494; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Security vulnerabilities in operating systems and firmware assessed as extreme risk are patched, updated or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent third parties, system managers or users.

Security Control: 1500; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
An automated mechanism is used to confirm and record that deployed operating system and firmware patches or updates have been installed, applied successfully and remain in place.

Security Control: 1501; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Operating systems for workstations, servers and ICT equipment that are no longer supported by vendors with patches or updates for security vulnerabilities are updated or replaced with vendor-supported versions.

Multi-factor authentication

Multi-factor authentication *including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.*

Security Control: 1173; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS
Multi-factor authentication is used to authenticate all privileged users and any other positions of trust.

Security Control: 1504; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Multi-factor authentication is used to authenticate all users of remote access solutions.

Security Control: 1505; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Multi-factor authentication is used to authenticate all users when accessing important data repositories.

Security Control: 1401; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.

Mitigation strategies to recover data and system availability

Daily backups

Daily backups *of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.*

Security Control: 1511; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Backups of important information, software and configuration settings are performed at least daily.

Security Control: 1512; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Backups are stored offline, or online but in a non-rewritable and non-erasable manner.

Security Control: 1514; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Backups are stored for three months or greater.

Security Control: 1515; Revision: 1; Updated: Jul-19; Applicability: O, P, S, TS
Full restoration of backups is tested at least once when initially implemented and each time fundamental information technology infrastructure changes occur.

Security Control: 1516; Revision: 1; Updated: Jul-19; Applicability: O, P, S, TS
Partial restoration of backups is tested on a quarterly or more frequent basis.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

The ***Essential Eight Maturity Model*** complements the advice in the ***Strategies to Mitigate Cyber Security Incidents***. It can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.