Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Essential Eight Maturity Model to ISM Mapping

First published: January 2019
Last updated: March 2023

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 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.

As the Essential Eight outlines a minimum set of preventative measures, organisations need to implement additional measures 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* (ISM).

Mapping the Essential Eight Maturity Model to the ISM

As the implementation of Maturity Level Two is the baseline for non-corporate Commonwealth entities, Maturity Level Two and Maturity Level Three of the *Essential Eight Maturity Model* have been mapped to the ISM below.

Maturity Level Two

Mitigation Strategy	Essential Eight Requirement	ISM Controls
Application control	Application control is implemented on workstations and internet-facing servers.	0843, 1490
	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	1657
	Allowed and blocked execution events on workstations and internet-facing servers are logged.	1660, 1661

Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	1807
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	1808
	A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.	1698
	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.	1699
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications.	1700
	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.	1690
	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.	1691
	Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month of release.	1693
	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.	1704
Configure Microsoft Office macro settings	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	1671
	Microsoft Office macros in files originating from the internet are blocked.	1488
	Microsoft Office macro antivirus scanning is enabled.	1672
	Microsoft Office macros are blocked from making Win32 API calls.	1673
	Microsoft Office macro security settings cannot be changed by users.	1489
	Allowed and blocked Microsoft Office macro execution events are logged.	1677
	Web browsers do not process Java from the internet.	1486

User application hardening	Web browsers do not process web advertisements from the internet.	1485
	Internet Explorer 11 does not process content from the internet.	1666
	Web browser security settings cannot be changed by users.	1585
	Microsoft Office is blocked from creating child processes.	1667
	Microsoft Office is blocked from creating executable content.	1668
	Microsoft Office is blocked from injecting code into other processes.	1669
	Microsoft Office is configured to prevent activation of OLE packages.	1542
	Microsoft Office security settings cannot be changed by users.	1823
	PDF software is blocked from creating child processes.	1670
	PDF software security settings cannot be changed by users.	1824
	ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.	1412
	Blocked PowerShell script execution events are logged.	1664
Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested.	1507
	Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.	1647
	Privileged access to systems and applications is automatically disabled after 45 days of inactivity.	1648
	Privileged accounts (excluding privileged service accounts) are prevented from accessing the internet, email and web services.	1175
	Privileged users use separate privileged and unprivileged operating environments.	1380
	Privileged operating environments are not virtualised within unprivileged operating environments.	1687
	Unprivileged accounts cannot logon to privileged operating environments.	1688

	Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	1689
	Administrative activities are conducted through jump servers.	1387
	Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed.	1685
	Privileged access events are logged.	1509
	Privileged account and group management events are logged.	1650
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.	1807
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	1808
	A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in operating systems of internet-facing services.	1701
	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.	1702
	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.	1694
	Patches, updates or vendor mitigations for security vulnerabilities in operating systems of workstations, servers and network devices are applied within two weeks of release.	1695
	Operating systems that are no longer supported by vendors are replaced.	1501
Multi-factor authentication	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation’s internet-facing services.	1504
	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.	1679
	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.	1680

	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.	1681
	Multi-factor authentication is used to authenticate privileged users of systems.	1173
	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.	1401
	Successful and unsuccessful multi-factor authentication events are logged.	1683
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.	1511
	Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time.	1810
	Backups of important data, software and configuration settings are retained in a secure and resilient manner.	1811
	Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises.	1515
	Unprivileged accounts cannot access backups belonging to other accounts.	1812
	Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts.	1705
	Unprivileged accounts are prevented from modifying and deleting backups.	1814
	Privileged accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups.	1707

Maturity Level Three

Mitigation Strategy	Essential Eight Requirement	ISM Controls
Application control	Application control is implemented on workstations and servers.	0843, 1490, 1656
	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.	1657, 1658

	Microsoft's 'recommended block rules' are implemented.	1544
	Microsoft's 'recommended driver block rules' are implemented.	1659
	Application control rulesets are validated on an annual or more frequent basis.	1582
	Allowed and blocked execution events on workstations and servers are centrally logged.	1660, 1661, 1662, 1663, 1405
	Event logs are protected from unauthorised modification and deletion.	1815
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	0109, 0123, 0140, 1228, 1819
Patch applications	An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities.	1807
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	1808
	A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in internet-facing services.	1698
	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.	1699
	A vulnerability scanner is used at least fortnightly to identify missing patches or updates for security vulnerabilities in other applications.	1700
	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.	1690
	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.	1691, 1692
	Patches, updates or vendor mitigations for security vulnerabilities in other applications are applied within one month of release.	1693
	Applications that are no longer supported by vendors are removed.	1704, 0304

Configure Microsoft Office macro settings	Microsoft Office macros are disabled for users that do not have a demonstrated business requirement.	1671
	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.	1674
	Only privileged users responsible for validating that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations.	1487
	Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View.	1675
	Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis.	1676
	Microsoft Office macros in files originating from the internet are blocked.	1488
	Microsoft Office macro antivirus scanning is enabled.	1672
	Microsoft Office macros are blocked from making Win32 API calls.	1673
	Microsoft Office macro security settings cannot be changed by users.	1489
	Allowed and blocked Microsoft Office macro execution events are centrally logged.	1677, 1678, 1405
	Event logs are protected from unauthorised modification and deletion.	1815
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	0109, 0123, 0140, 1228, 1819
User application hardening	Web browsers do not process Java from the internet.	1486
	Web browsers do not process web advertisements from the internet.	1485
	Internet Explorer 11 is disabled or removed.	1654
	Web browser security settings cannot be changed by users.	1585
	Microsoft Office is blocked from creating child processes.	1667
	Microsoft Office is blocked from creating executable content.	1668

	Microsoft Office is blocked from injecting code into other processes.	1669
	Microsoft Office is configured to prevent activation of OLE packages.	1542
	Microsoft Office security settings cannot be changed by users.	1823
	PDF software is blocked from creating child processes.	1670
	PDF software security settings cannot be changed by users.	1824
	ACSC or vendor hardening guidance for web browsers, Microsoft Office and PDF software is implemented.	1412
	.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.	1655
	Windows PowerShell 2.0 is disabled or removed.	1621
	PowerShell is configured to use Constrained Language Mode.	1622
	Blocked PowerShell script execution events are centrally logged.	1664, 1665, 1405
	Event logs are protected from unauthorised modification and deletion.	1815
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	0109, 0123, 0140, 1228, 1819
Restrict administrative privileges	Requests for privileged access to systems and applications are validated when first requested.	1507
	Privileged access to systems and applications is automatically disabled after 12 months unless revalidated.	1647
	Privileged access to systems and applications is automatically disabled after 45 days of inactivity.	1648
	Privileged access to systems and applications is limited to only what is required for users and services to undertake their duties.	1508
	Privileged accounts are prevented from accessing the internet, email and web services.	1175, 1653
	Privileged users use separate privileged and unprivileged operating environments.	1380

	Privileged operating environments are not virtualised within unprivileged operating environments.	1687
	Unprivileged accounts cannot logon to privileged operating environments.	1688
	Privileged accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments.	1689
	Just-in-time administration is used for administering systems and applications.	1649
	Administrative activities are conducted through jump servers.	1387
	Credentials for local administrator accounts and service accounts are long, unique, unpredictable and managed.	1685
	Windows Defender Credential Guard and Windows Defender Remote Credential Guard are enabled.	1686
	Privileged access events are centrally logged.	1509, 1651, 1405
	Privileged account and group management events are centrally logged.	1650, 1652, 1405
	Event logs are protected from unauthorised modification and deletion.	1815
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	0109, 0123, 0140, 1228, 1819
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.	1807
	A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities.	1808
	A vulnerability scanner is used at least daily to identify missing patches or updates for security vulnerabilities in operating systems of internet-facing services.	1701
	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.	1702

	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.	1694
	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.	1695, 1696
	The latest release, or the previous release, of operating systems are used.	1407
	Operating systems that are no longer supported by vendors are replaced.	1501
Multi-factor authentication	Multi-factor authentication is used by an organisation's users if they authenticate to their organisation's internet-facing services.	1504
	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.	1679
	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.	1680
	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.	1681
	Multi-factor authentication is used to authenticate privileged users of systems.	1173
	Multi-factor authentication is used to authenticate users accessing important data repositories.	1505
	Multi-factor authentication is phishing-resistant and uses either: something users have and something users know, or something users have that is unlocked by something users know or are.	1401, 1682
	Successful and unsuccessful multi-factor authentication events are centrally logged.	1683, 1684, 1405
	Event logs are protected from unauthorised modification and deletion.	1815
	Event logs are monitored for signs of compromise and actioned when any signs of compromise are detected.	0109, 0123, 0140, 1228, 1819

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.	1511
	Backups of important data, software and configuration settings are synchronised to enable restoration to a common point in time.	1810
	Backups of important data, software and configuration settings are retained in a secure and resilient manner.	1811
	Restoration of important data, software and configuration settings from backups to a common point in time is tested as part of disaster recovery exercises.	1515
	Unprivileged accounts cannot access backups belonging to other accounts, nor their own accounts.	1812, 1813
	Privileged accounts (excluding backup administrator accounts) cannot access backups belonging to other accounts, nor their own accounts.	1705, 1706
	Unprivileged accounts are prevented from modifying and deleting backups.	1814
	Privileged accounts (including backup administrator accounts) are prevented from modifying and deleting backups during their retention period.	1707, 1708

Further information

The *Information Security Manual* is a cyber security framework that organisations can apply to protect their systems and data from cyber threats. The advice in the *Strategies to Mitigate Cyber Security Incidents*, along with its Essential Eight, complements this framework.

Contact details

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