



Essential Eight maturity model and ISM mapping

First published: January 2019
Last updated: October 2024

Introduction

The Australian Signals Directorate (ASD) has developed prioritised mitigation strategies, in the form of the [Strategies to mitigate cybersecurity incidents](#), to help organisations protect themselves against various cyberthreats. 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 ASD's experience in producing cyberthreat intelligence, responding to cybersecurity incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.

This publication provides a mapping between the [Essential Eight maturity model](#) and the [Information security manual](#) (ISM).

Mapping between the *Essential Eight maturity model* and the ISM

Maturity Level One

| Mitigation Strategy | Essential Eight Requirement | ISM Control |
|---------------------|--|-------------|
| Patch applications | An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. | ISM-1807 |
| | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | ISM-1808 |
| | A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services. | ISM-1698 |
| | A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. | ISM-1699 |

| | |
|---|----------|
| Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | ISM-1876 |
|---|----------|

| | |
|---|----------|
| Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | ISM-1690 |
|---|----------|

| | |
|--|----------|
| Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release. | ISM-1691 |
|--|----------|

| | |
|--|----------|
| Online services that are no longer supported by vendors are removed. | ISM-1905 |
|--|----------|

| | |
|--|----------|
| 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. | ISM-1704 |
|--|----------|

| | | |
|--------------------------------|--|----------|
| 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. | ISM-1807 |
|--------------------------------|--|----------|

| | |
|--|----------|
| A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | ISM-1808 |
|--|----------|

| | |
|--|----------|
| A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices. | ISM-1701 |
|--|----------|

| | |
|--|----------|
| A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices. | ISM-1702 |
|--|----------|

| | |
|--|----------|
| Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | ISM-1877 |
|--|----------|

| | |
|--|----------|
| Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | ISM-1694 |
|--|----------|

| | |
|---|----------|
| Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release. | ISM-1695 |
|---|----------|

| | |
|---|----------|
| Operating systems that are no longer supported by vendors are replaced. | ISM-1501 |
|---|----------|

| | | |
|---|---|----------|
| Multi-factor authentication | Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data. | ISM-1504 |
| | Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data. | ISM-1679 |
| | Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data. | ISM-1680 |
| | Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data. | ISM-1892 |
| | Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data. | ISM-1893 |
| | Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data. | ISM-1681 |
| | 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. | ISM-1401 |
| Restrict administrative privileges | Requests for privileged access to systems, applications and data repositories are validated when first requested. | ISM-1507 |
| | Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access. | ISM-0445 |
| | Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services. | ISM-1175 |
| | Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties. | ISM-1883 |
| | Privileged users use separate privileged and unprivileged operating environments. | ISM-1380 |
| | Unprivileged user accounts cannot logon to privileged operating environments. | ISM-1688 |

| | | |
|---|--|----------|
| | Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. | ISM-1689 |
| Application control | Application control is implemented on workstations. | ISM-0843 |
| | Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients. | ISM-1870 |
| | Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set. | ISM-1657 |
| Restrict Microsoft Office macros | Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. | ISM-1671 |
| | Microsoft Office macros in files originating from the internet are blocked. | ISM-1488 |
| | Microsoft Office macro antivirus scanning is enabled. | ISM-1672 |
| | Microsoft Office macro security settings cannot be changed by users. | ISM-1489 |
| User application hardening | Internet Explorer 11 is disabled or removed. | ISM-1654 |
| | Web browsers do not process Java from the internet. | ISM-1486 |
| | Web browsers do not process web advertisements from the internet. | ISM-1485 |
| | Web browser security settings cannot be changed by users. | ISM-1585 |
| Regular backups | Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements. | ISM-1511 |
| | Backups of data, applications and settings are synchronised to enable restoration to a common point in time. | ISM-1810 |
| | Backups of data, applications and settings are retained in a secure and resilient manner. | ISM-1811 |
| | Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises. | ISM-1515 |
| | Unprivileged user accounts cannot access backups belonging to other user accounts. | ISM-1812 |
| | Unprivileged user accounts are prevented from modifying and deleting backups. | ISM-1814 |

Maturity Level Two

| Mitigation Strategy | Essential Eight Requirement | ISM Control |
|---------------------------|---|-------------|
| Patch applications | An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. | ISM-1807 |
| | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | ISM-1808 |
| | A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services. | ISM-1698 |
| | A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. | ISM-1699 |
| | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. | ISM-1700 |
| | Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | ISM-1876 |
| | Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | ISM-1690 |
| | Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release. | ISM-1691 |
| | Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. | ISM-1693 |
| | Online services that are no longer supported by vendors are removed. | ISM-1905 |
| | 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. | ISM-1704 |

| | | |
|------------------------------------|--|----------|
| 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. | ISM-1807 |
| | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | ISM-1808 |
| | A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices. | ISM-1701 |
| | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices. | ISM-1702 |
| | Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | ISM-1877 |
| | Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | ISM-1694 |
| | Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release. | ISM-1695 |
| | Operating systems that are no longer supported by vendors are replaced. | ISM-1501 |
| Multi-factor authentication | Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data. | ISM-1504 |
| | Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data. | ISM-1679 |
| | Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data. | ISM-1680 |
| | Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data. | ISM-1892 |

| | |
|--|----------|
| Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data. | ISM-1893 |
| Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data. | ISM-1681 |
| Multi-factor authentication is used to authenticate privileged users of systems. | ISM-1173 |
| Multi-factor authentication is used to authenticate unprivileged users of systems. | ISM-0974 |
| 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. | ISM-1401 |
| Multi-factor authentication used for authenticating users of online services is phishing-resistant. | ISM-1872 |
| Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option. | ISM-1873 |
| Multi-factor authentication used for authenticating users of systems is phishing-resistant. | ISM-1682 |
| Successful and unsuccessful multi-factor authentication events are centrally logged. | ISM-1683 |
| Event logs are protected from unauthorised modification and deletion. | ISM-1815 |
| Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | ISM-1906 |
| Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | ISM-1228 |
| Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | ISM-0123 |
| Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | ISM-0140 |
| Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | ISM-1819 |

| | | |
|---|--|----------|
| Restrict administrative privileges | Requests for privileged access to systems, applications and data repositories are validated when first requested. | ISM-1507 |
| | Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated. | ISM-1647 |
| | Privileged access to systems and applications is disabled after 45 days of inactivity. | ISM-1648 |
| | Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access. | ISM-0445 |
| | Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services. | ISM-1175 |
| | Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties. | ISM-1883 |
| | Privileged users use separate privileged and unprivileged operating environments. | ISM-1380 |
| | Privileged operating environments are not virtualised within unprivileged operating environments. | ISM-1687 |
| | Unprivileged user accounts cannot logon to privileged operating environments. | ISM-1688 |
| | Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. | ISM-1689 |
| | Administrative activities are conducted through jump servers. | ISM-1387 |
| | Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed. | ISM-1685 |
| | Privileged access events are centrally logged. | ISM-1509 |
| | Privileged user account and security group management events are centrally logged. | ISM-1650 |
| | Event logs are protected from unauthorised modification and deletion. | ISM-1815 |
| | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | ISM-1906 |
| | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | ISM-1228 |

| | | |
|----------------------------|--|----------|
| | Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | ISM-0123 |
| | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | ISM-0140 |
| | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | ISM-1819 |
| Application control | Application control is implemented on workstations. | ISM-0843 |
| | Application control is implemented on internet-facing servers. | ISM-1490 |
| | Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients. | ISM-1870 |
| | Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients. | ISM-1871 |
| | Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set. | ISM-1657 |
| | Microsoft's recommended application blocklist is implemented. | ISM-1544 |
| | Application control rulesets are validated on an annual or more frequent basis. | ISM-1582 |
| | Allowed and blocked application control events are centrally logged. | ISM-1660 |
| | Event logs are protected from unauthorised modification and deletion. | ISM-1815 |
| | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | ISM-1906 |
| | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | ISM-1228 |
| | Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | ISM-0123 |
| | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | ISM-0140 |
| | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | ISM-1819 |

| | | |
|---|---|----------|
| Restrict Microsoft Office macros | Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. | ISM-1671 |
| | Microsoft Office macros in files originating from the internet are blocked. | ISM-1488 |
| | Microsoft Office macro antivirus scanning is enabled. | ISM-1672 |
| | Microsoft Office macros are blocked from making Win32 API calls. | ISM-1673 |
| | Microsoft Office macro security settings cannot be changed by users. | ISM-1489 |
| User application hardening | Internet Explorer 11 is disabled or removed. | ISM-1654 |
| | Web browsers do not process Java from the internet. | ISM-1486 |
| | Web browsers do not process web advertisements from the internet. | ISM-1485 |
| | Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | ISM-1412 |
| | Web browser security settings cannot be changed by users. | ISM-1585 |
| | Microsoft Office is blocked from creating child processes. | ISM-1667 |
| | Microsoft Office is blocked from creating executable content. | ISM-1668 |
| | Microsoft Office is blocked from injecting code into other processes. | ISM-1669 |
| | Microsoft Office is configured to prevent activation of Object Linking and Embedding packages. | ISM-1542 |
| | Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | ISM-1859 |
| | Office productivity suite security settings cannot be changed by users. | ISM-1823 |
| | PDF software is blocked from creating child processes. | ISM-1670 |
| | PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | ISM-1860 |
| | PDF software security settings cannot be changed by users. | ISM-1824 |

| | | |
|------------------------|--|----------|
| | PowerShell module logging, script block logging and transcription events are centrally logged. | ISM-1623 |
| | Command line process creation events are centrally logged. | ISM-1889 |
| | Event logs are protected from unauthorised modification and deletion. | ISM-1815 |
| | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | ISM-1906 |
| | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | ISM-1228 |
| | Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | ISM-0123 |
| | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | ISM-0140 |
| | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | ISM-1819 |
| Regular backups | Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements. | ISM-1511 |
| | Backups of data, applications and settings are synchronised to enable restoration to a common point in time. | ISM-1810 |
| | Backups of data, applications and settings are retained in a secure and resilient manner. | ISM-1811 |
| | Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises. | ISM-1515 |
| | Unprivileged user accounts cannot access backups belonging to other user accounts. | ISM-1812 |
| | Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts. | ISM-1705 |
| | Unprivileged user accounts are prevented from modifying and deleting backups. | ISM-1814 |
| | Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups. | ISM-1707 |

Maturity Level Three

| Mitigation Strategy | Essential Eight Requirement | ISM Control |
|---------------------|---|-------------|
| Patch applications | An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. | ISM-1807 |
| | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | ISM-1808 |
| | A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services. | ISM-1698 |
| | A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. | ISM-1699 |
| | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products. | ISM-1700 |
| | Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | ISM-1876 |
| | Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | ISM-1690 |
| | Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | ISM-1692 |
| | Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | ISM-1901 |
| | Patches, updates or other vendor mitigations for vulnerabilities in applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products are applied within one month of release. | ISM-1693 |

| | | |
|--------------------------------|--|----------|
| | Online services that are no longer supported by vendors are removed. | ISM-1905 |
| | 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. | ISM-1704 |
| | Applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, Adobe Flash Player, and security products that are no longer supported by vendors are removed. | ISM-0304 |
| 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. | ISM-1807 |
| | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | ISM-1808 |
| | A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices. | ISM-1701 |
| | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices. | ISM-1702 |
| | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers. | ISM-1703 |
| | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware. | ISM-1900 |
| | Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | ISM-1877 |
| | Patches, updates or other vendor mitigations for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices are applied within two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | ISM-1694 |
| | Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | ISM-1696 |

| | | |
|------------------------------------|--|----------|
| | Patches, updates or other vendor mitigations for vulnerabilities in operating systems of workstations, non-internet-facing servers and non-internet-facing network devices are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | ISM-1902 |
| | Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | ISM-1879 |
| | Patches, updates or other vendor mitigations for vulnerabilities in drivers are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | ISM-1697 |
| | Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within 48 hours of release when vulnerabilities are assessed as critical by vendors or when working exploits exist. | ISM-1903 |
| | Patches, updates or other vendor mitigations for vulnerabilities in firmware are applied within one month of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | ISM-1904 |
| | The latest release, or the previous release, of operating systems are used. | ISM-1407 |
| | Operating systems that are no longer supported by vendors are replaced. | ISM-1501 |
| Multi-factor authentication | Multi-factor authentication is used to authenticate users to their organisation's online services that process, store or communicate their organisation's sensitive data. | ISM-1504 |
| | Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data. | ISM-1679 |
| | Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organisation's non-sensitive data. | ISM-1680 |
| | Multi-factor authentication is used to authenticate users to their organisation's online customer services that process, store or communicate their organisation's sensitive customer data. | ISM-1892 |
| | Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organisation's sensitive customer data. | ISM-1893 |

| | |
|--|----------|
| Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data. | ISM-1681 |
| Multi-factor authentication is used to authenticate privileged users of systems. | ISM-1173 |
| Multi-factor authentication is used to authenticate unprivileged users of systems. | ISM-0974 |
| Multi-factor authentication is used to authenticate users of data repositories. | ISM-1505 |
| 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. | ISM-1401 |
| Multi-factor authentication used for authenticating users of online services is phishing-resistant. | ISM-1872 |
| Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant. | ISM-1874 |
| Multi-factor authentication used for authenticating users of systems is phishing-resistant. | ISM-1682 |
| Multi-factor authentication used for authenticating users of data repositories is phishing-resistant. | ISM-1894 |
| Successful and unsuccessful multi-factor authentication events are centrally logged. | ISM-1683 |
| Event logs are protected from unauthorised modification and deletion. | ISM-1815 |
| Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | ISM-1906 |
| Event logs from non-internet-facing servers are analysed in a timely manner to detect cybersecurity events. | ISM-1907 |
| Event logs from workstations are analysed in a timely manner to detect cybersecurity events. | ISM-0109 |
| Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | ISM-1228 |
| Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | ISM-0123 |

| | | |
|---|--|----------|
| | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | ISM-0140 |
| | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | ISM-1819 |
| Restrict administrative privileges | Requests for privileged access to systems, applications and data repositories are validated when first requested. | ISM-1507 |
| | Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated. | ISM-1647 |
| | Privileged access to systems and applications is disabled after 45 days of inactivity. | ISM-1648 |
| | Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access. | ISM-0445 |
| | Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties. | ISM-1508 |
| | Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services. | ISM-1175 |
| | Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to undertake their duties. | ISM-1883 |
| | Secure Admin Workstations are used in the performance of administrative activities. | ISM-1898 |
| | Privileged users use separate privileged and unprivileged operating environments. | ISM-1380 |
| | Privileged operating environments are not virtualised within unprivileged operating environments. | ISM-1687 |
| | Unprivileged user accounts cannot logon to privileged operating environments. | ISM-1688 |
| | Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. | ISM-1689 |
| | Just-in-time administration is used for administering systems and applications. | ISM-1649 |
| | Administrative activities are conducted through jump servers. | ISM-1387 |

| | | |
|--|--|----------|
| Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed. | ISM-1685 | |
| Memory integrity functionality is enabled. | ISM-1896 | |
| Local Security Authority protection functionality is enabled. | ISM-1861 | |
| Credential Guard functionality is enabled. | ISM-1686 | |
| Remote Credential Guard functionality is enabled. | ISM-1897 | |
| Privileged access events are centrally logged. | ISM-1509 | |
| Privileged user account and security group management events are centrally logged. | ISM-1650 | |
| Event logs are protected from unauthorised modification and deletion. | ISM-1815 | |
| Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | ISM-1906 | |
| Event logs from non-internet-facing servers are analysed in a timely manner to detect cybersecurity events. | ISM-1907 | |
| Event logs from workstations are analysed in a timely manner to detect cybersecurity events. | ISM-0109 | |
| Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | ISM-1228 | |
| Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | ISM-0123 | |
| Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | ISM-0140 | |
| Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | ISM-1819 | |
| Application control | Application control is implemented on workstations. | ISM-0843 |
| | Application control is implemented on internet-facing servers. | ISM-1490 |
| | Application control is implemented on non-internet-facing servers. | ISM-1656 |
| | Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients. | ISM-1870 |

| | | |
|---|--|----------|
| | Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients. | ISM-1871 |
| | Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set. | ISM-1657 |
| | Application control restricts the execution of drivers to an organisation-approved set. | ISM-1658 |
| | Microsoft's recommended application blocklist is implemented. | ISM-1544 |
| | Microsoft's vulnerable driver blocklist is implemented. | ISM-1659 |
| | Application control rulesets are validated on an annual or more frequent basis. | ISM-1582 |
| | Allowed and blocked application control events are centrally logged. | ISM-1660 |
| | Event logs are protected from unauthorised modification and deletion. | ISM-1815 |
| | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | ISM-1906 |
| | Event logs from non-internet-facing servers are analysed in a timely manner to detect cybersecurity events. | ISM-1907 |
| | Event logs from workstations are analysed in a timely manner to detect cybersecurity events. | ISM-0109 |
| | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | ISM-1228 |
| | Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | ISM-0123 |
| | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | ISM-0140 |
| | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | ISM-1819 |
| Restrict Microsoft Office macros | Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. | ISM-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. | ISM-1674 |
| | Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations. | ISM-1890 |
| | Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations. | ISM-1487 |
| | Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View. | ISM-1675 |
| | Microsoft Office macros digitally signed by signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View. | ISM-1891 |
| | Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis. | ISM-1676 |
| | Microsoft Office macros in files originating from the internet are blocked. | ISM-1488 |
| | Microsoft Office macro antivirus scanning is enabled. | ISM-1672 |
| | Microsoft Office macros are blocked from making Win32 API calls. | ISM-1673 |
| | Microsoft Office macro security settings cannot be changed by users. | ISM-1489 |
| User application hardening | Internet Explorer 11 is disabled or removed. | ISM-1654 |
| | Web browsers do not process Java from the internet. | ISM-1486 |
| | Web browsers do not process web advertisements from the internet. | ISM-1485 |
| | Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | ISM-1412 |
| | Web browser security settings cannot be changed by users. | ISM-1585 |
| | Microsoft Office is blocked from creating child processes. | ISM-1667 |
| | Microsoft Office is blocked from creating executable content. | ISM-1668 |
| | Microsoft Office is blocked from injecting code into other processes. | ISM-1669 |

| | |
|--|----------|
| Microsoft Office is configured to prevent activation of Object Linking and Embedding packages. | ISM-1542 |
| Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | ISM-1859 |
| Office productivity suite security settings cannot be changed by users. | ISM-1823 |
| PDF software is blocked from creating child processes. | ISM-1670 |
| PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | ISM-1860 |
| PDF software security settings cannot be changed by users. | ISM-1824 |
| .NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed. | ISM-1655 |
| Windows PowerShell 2.0 is disabled or removed. | ISM-1621 |
| PowerShell is configured to use Constrained Language Mode. | ISM-1622 |
| PowerShell module logging, script block logging and transcription events are centrally logged. | ISM-1623 |
| Command line process creation events are centrally logged. | ISM-1889 |
| Event logs are protected from unauthorised modification and deletion. | ISM-1815 |
| Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | ISM-1906 |
| Event logs from non-internet-facing servers are analysed in a timely manner to detect cybersecurity events. | ISM-1907 |
| Event logs from workstations are analysed in a timely manner to detect cybersecurity events. | ISM-0109 |
| Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | ISM-1228 |
| Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | ISM-0123 |
| Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | ISM-0140 |

| | | |
|------------------------|---|----------|
| | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | ISM-1819 |
| Regular backups | Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements. | ISM-1511 |
| | Backups of data, applications and settings are synchronised to enable restoration to a common point in time. | ISM-1810 |
| | Backups of data, applications and settings are retained in a secure and resilient manner. | ISM-1811 |
| | Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises. | ISM-1515 |
| | Unprivileged user accounts cannot access backups belonging to other user accounts. | ISM-1812 |
| | Unprivileged user accounts cannot access their own backups. | ISM-1813 |
| | Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts. | ISM-1705 |
| | Privileged user accounts (excluding backup administrator accounts) cannot access their own backups. | ISM-1706 |
| | Unprivileged user accounts are prevented from modifying and deleting backups. | ISM-1814 |
| | Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups. | ISM-1707 |
| | Backup administrator accounts are prevented from modifying and deleting backups during their retention period. | ISM-1708 |

Further information

The [Information security manual](#) is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the [Strategies to mitigate cybersecurity 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).

Disclaimer

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

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

Copyright

© Commonwealth of Australia 2024.

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

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



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

Use of the Coat of Arms

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

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

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



Australian Government
Australian Signals Directorate