

NIST IR 8477-Based Set Theory Relationship Mapping (STRM)

Reference document: Secure Controls Framework (SCF) version 2026.1
STRM Guidance: <https://securecontrolsframework.com/set-theory-relationship-mapping-strm/>

Focal Document:

Focal Document URL:
Published STRM URL:

Australia -Essential Eight maturity model and ISM mapping (2024)

<https://www.cyber.gov.au/business-governments/australian-cyber-security-framework/essential-eight-maturity-model-and-ism-mapping>
<https://content.securecontrolsframework.com/set-theory-relationship-mapping-strm-ess-e8-2024.pdf>

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes |
|--------|------------------------------------|--|----------------|-------------------|--|----------|---|--------------------------|----------|
| ML1-P1 | Patch applications | An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. | Functional | Subset Of | Asset Inventories | AST-02 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel. | 10 | ISM-1807 |
| ML1-P1 | Patch applications | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | Functional | Intersects With | Update Tool Capability | VPM-06.1 | Mechanisms exist to update vulnerability scanning tools. | 8 | ISM-1808 |
| ML1-P1 | Patch applications | A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1698 |
| ML1-P1 | Patch applications | 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. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1699 |
| ML1-P1 | Patch applications | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1876 |
| ML1-P1 | Patch applications | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1690 |
| ML1-P1 | Patch applications | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1691 |
| ML1-P1 | Patch applications | Online services that are no longer supported by vendors are removed. | Functional | Subset Of | Unsupported Technology Assets, Applications and/or Services (TAAS) | TDA-17 | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs. | 10 | ISM-1905 |
| ML1-P1 | Patch applications | 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. | Functional | Subset Of | Unsupported Technology Assets, Applications and/or Services (TAAS) | TDA-17 | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs. | 10 | ISM-1704 |
| ML1-P2 | 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. | Functional | Subset Of | Asset Inventories | AST-02 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel. | 10 | ISM-1807 |
| ML1-P2 | Patch operating systems | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | Functional | Intersects With | Update Tool Capability | VPM-06.1 | Mechanisms exist to update vulnerability scanning tools. | 8 | ISM-1808 |
| ML1-P2 | Patch operating systems | 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. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1701 |
| ML1-P2 | Patch operating systems | 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. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1702 |
| ML1-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1877 |
| ML1-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1694 |
| ML1-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1695 |
| ML1-P2 | Patch operating systems | Operating systems that are no longer supported by vendors are replaced. | Functional | Subset Of | Unsupported Technology Assets, Applications and/or Services (TAAS) | TDA-17 | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs. | 10 | ISM-1501 |
| ML1-P3 | 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. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1504 |
| ML1-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1679 |
| ML1-P3 | Multi-factor authentication | 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. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1680 |
| ML1-P3 | Multi-factor authentication | 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. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1892 |
| ML1-P3 | Multi-factor authentication | 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. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1893 |
| ML1-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1681 |
| ML1-P3 | Multi-factor authentication | Multi-factor authentication users either: something users have and something users know, or something users have that is unlocked by something users know or are. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1401 |
| ML1-P4 | Restrict administrative privileges | Requests for privileged access to systems, applications and data repositories are validated when first requested. | Functional | Intersects With | Privileged Account Management (PAM) | IAC-16 | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS). | 5 | ISM-1507 |
| ML1-P4 | Restrict administrative privileges | Requests for privileged access to systems, applications and data repositories are validated when first requested. | Functional | Intersects With | Management Approval For Privileged Accounts | IAC-21.3 | Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles. | 5 | ISM-1507 |
| ML1-P4 | Restrict administrative privileges | Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access. | Functional | Equal | Dedicated Privileged Account | IAC-16.4 | Mechanisms exist to assign dedicated privileged user accounts to be used solely for specific roles with legitimate business needs. | 10 | ISM-1445 |
| ML1-P4 | Restrict administrative privileges | Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services. | Functional | Intersects With | Non-Privileged Access For Non-Security Functions | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions. | 5 | ISM-1775 |
| ML1-P4 | Restrict administrative privileges | 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. | Functional | Subset Of | Least Privilege | IAC-21 | Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions. | 10 | ISM-1883 |
| ML1-P4 | Restrict administrative privileges | Privileged users use separate privileged and unprivileged operating environments. | Functional | Intersects With | Privileged Account Management (PAM) | IAC-16 | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS). | 5 | ISM-1380 |
| ML1-P4 | Restrict administrative privileges | Unprivileged user accounts cannot logon to privileged operating environments. | Functional | Subset Of | Role-Based Access Control (RBAC) | IAC-08 | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs. | 10 | ISM-1688 |
| ML1-P4 | Restrict administrative privileges | Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. | Functional | Intersects With | Non-Privileged Access For Non-Security Functions | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions. | 5 | ISM-1689 |
| ML1-P5 | Application control | Application control is implemented on workstations. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 8 | ISM-0843 |
| ML1-P5 | Application control | Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 5 | ISM-1870 |
| ML1-P5 | Application control | Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved user set. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 5 | ISM-1657 |
| ML1-P6 | Restrict Microsoft Office macros | Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1671 |
| ML1-P6 | Restrict Microsoft Office macros | Microsoft Office macros in files originating from the internet are blocked. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1488 |
| ML1-P6 | Restrict Microsoft Office macros | Microsoft Office macro antivirus scanning is enabled. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1672 |
| ML1-P6 | Restrict Microsoft Office macros | Microsoft Office macro security settings cannot be changed by users. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1489 |
| ML1-P7 | User application hardening | Internet Explorer 11 is disabled or removed. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1654 |
| ML1-P7 | User application hardening | Web browsers do not process Java from the internet. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1486 |
| ML1-P7 | User application hardening | Web browsers do not process web advertisements from the internet. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1485 |
| ML1-P7 | User application hardening | Web browser security settings cannot be changed by users. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1585 |
| ML1-P8 | Regular backups | Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements. | Functional | Intersects With | Data Backups | BCD-11 | Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). | 5 | ISM-1511 |
| ML1-P8 | Regular backups | Backups of data, applications and settings are synchronized to enable restoration to a common point in time. | Functional | Intersects With | Recovery Time / Point Objectives (RTO / RPO) | BCD-01.4 | Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). | 5 | ISM-1810 |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes |
|--------|-----------------------------|--|----------------|-------------------|--|-----------|---|--------------------------|----------|
| ML1-P8 | Regular backups | Backups of data, applications and settings are retained in a secure and resilient manner. | Functional | Intersects With | Separate Storage for Critical Information | BCD-11.2 | Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up. | 5 | ISM-1811 |
| ML1-P8 | Regular backups | Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises. | Functional | Intersects With | Test Restoration Using Sampling | BCD-11.5 | Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing. | 5 | ISM-1515 |
| ML1-P8 | Regular backups | Unprivileged user accounts cannot access backups belonging to other user accounts. | Functional | Intersects With | Backup Access | BCD-11.9 | Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations. | 5 | ISM-1812 |
| ML1-P8 | Regular backups | Unprivileged user accounts are prevented from modifying and deleting backups. | Functional | Intersects With | Backup Modification and/or Destruction | BCD-11.10 | Mechanisms exist to restrict access to modify and/or delete backups to privileged users with assigned data backup and recovery operations roles. | 5 | ISM-1814 |
| ML2-P1 | Patch applications | An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. | Functional | Subset Of | Asset Inventories | AST-02 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel. | 10 | ISM-1807 |
| ML2-P1 | Patch applications | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | Functional | Intersects With | Update Tool Capability | VPM-06.1 | Mechanisms exist to update vulnerability scanning tools. | 8 | ISM-1808 |
| ML2-P1 | Patch applications | A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1698 |
| ML2-P1 | Patch applications | 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. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1699 |
| ML2-P1 | Patch applications | 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. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1700 |
| ML2-P1 | Patch applications | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1876 |
| ML2-P1 | Patch applications | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1690 |
| ML2-P1 | Patch applications | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1691 |
| ML2-P1 | Patch applications | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1693 |
| ML2-P1 | Patch applications | Online services that are no longer supported by vendors are removed. | Functional | Subset Of | Unsupported Technology Assets, Applications and/or Services (TAAS) | TDA-17 | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs. | 10 | ISM-1905 |
| ML2-P1 | Patch applications | 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. | Functional | Subset Of | Unsupported Technology Assets, Applications and/or Services (TAAS) | TDA-17 | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs. | 10 | ISM-1704 |
| ML2-P2 | 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. | Functional | Subset Of | Asset Inventories | AST-02 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel. | 10 | ISM-1807 |
| ML2-P2 | Patch operating systems | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | Functional | Intersects With | Update Tool Capability | VPM-06.1 | Mechanisms exist to update vulnerability scanning tools. | 8 | ISM-1808 |
| ML2-P2 | Patch operating systems | 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. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1701 |
| ML2-P2 | Patch operating systems | 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. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1702 |
| ML2-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1877 |
| ML2-P2 | Patch operating systems | 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 two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exploits exist. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1694 |
| ML2-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1695 |
| ML2-P2 | Patch operating systems | Operating systems that are no longer supported by vendors are replaced. | Functional | Subset Of | Unsupported Technology Assets, Applications and/or Services (TAAS) | TDA-17 | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs. | 10 | ISM-1501 |
| ML2-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate users to their organization's online services that process, store or communicate their organization's sensitive data. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1504 |
| ML2-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organization's sensitive data. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1679 |
| ML2-P3 | Multi-factor authentication | Multi-factor authentication (where available) is used to authenticate users to third-party online services that process, store or communicate their organization's non-sensitive data. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1680 |
| ML2-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate users to their organization's online customer services that process, store or communicate their organization's sensitive customer data. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1892 |
| ML2-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate users to third-party online customer services that process, store or communicate their organization's sensitive customer data. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1893 |
| ML2-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1681 |
| ML2-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate privileged users of systems. | Functional | Intersects With | Local Access to Privileged Accounts | IAC-06.3 | Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts. | 8 | ISM-1173 |
| ML2-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate unprivileged users of systems. | Functional | Intersects With | Network Access to Non-Privileged Accounts | IAC-06.2 | Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts. | 8 | ISM-0974 |
| ML2-P3 | Multi-factor authentication | 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. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1401 |
| ML2-P3 | Multi-factor authentication | Multi-factor authentication used for authenticating users of online services is phishing-resistant. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1872 |
| ML2-P3 | Multi-factor authentication | Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | Functional | Intersects With | Event Log Analysis & Triage | MON-17 | Mechanisms exist to ensure event log reviews include analysis and triage practices that integrate with the organization's established incident response processes. | 5 | ISM-0123 |
| ML2-P3 | Multi-factor authentication | Multi-factor authentication used for authenticating customers of online customer services provides a phishing-resistant option. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1873 |
| ML2-P3 | Multi-factor authentication | Multi-factor authentication used for authenticating users of systems is phishing-resistant. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1682 |
| ML2-P3 | Multi-factor authentication | Successful and unsuccessful multi-factor authentication events are centrally logged. | Functional | Intersects With | Content of Event Logs | MON-03 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event. | 5 | ISM-1683 |
| ML2-P3 | Multi-factor authentication | Event logs are protected from unauthorised modification and deletion. | Functional | Subset Of | Protection of Event Logs | MON-08 | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion. | 10 | ISM-1815 |
| ML2-P3 | Multi-factor authentication | Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1906 |
| ML2-P3 | Multi-factor authentication | Cyber security events are analysed in a timely manner to identify cyber security incidents. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1228 |
| ML2-P3 | Multi-factor authentication | Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | Functional | Intersects With | Event Log Analysis & Triage | MON-17 | Mechanisms exist to ensure event log reviews include analysis and triage practices that integrate with the organization's established incident response processes. | 5 | ISM-0123 |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes |
|--------|------------------------------------|---|----------------|-------------------|--|----------|--|--------------------------|----------|
| ML2-P3 | Multi-factor authentication | Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered. | Functional | Subset Of | Incident Stakeholder Reporting | IRO-10 | Mechanisms exist to timely-report incidents to applicable: 1) Internal stakeholders; 2) affected clients & third-parties; and 3) Regulatory authorities. | 10 | ISM-0140 |
| ML2-P3 | Multi-factor authentication | Following the identification of a cyber security incident, the cyber security incident response plan is enacted. | Functional | Subset Of | Incident Handling | IRO-02 | Mechanisms exist to cover: 1) Preparation; 2) Automated event detection or manual incident report intake; 3) Analysis; 4) Containment; 5) Eradication; and 6) Recovery. | 10 | ISM-1819 |
| ML2-P4 | Restrict administrative privileges | Requests for privileged access to systems, applications and data repositories are validated when first requested. | Functional | Intersects With | Privileged Account Management (PAM) | IAC-16 | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS). | 5 | ISM-1507 |
| ML2-P4 | Restrict administrative privileges | Requests for privileged access to systems, applications and data repositories are validated when first requested. | Functional | Intersects With | Management Approval For Privileged Accounts | IAC-21.3 | Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles. | 5 | ISM-1507 |
| ML2-P4 | Restrict administrative privileges | Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated. | Functional | Intersects With | Privileged Account Management (PAM) | IAC-16 | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS). | 3 | ISM-1647 |
| ML2-P4 | Restrict administrative privileges | Privileged access to systems and applications is disabled after 45 days of account inactivity. | Functional | Intersects With | Disable Inactive Accounts | IAC-15.3 | Automated mechanisms exist to disable inactive accounts after an organization defined time period. | 8 | ISM-1648 |
| ML2-P4 | Restrict administrative privileges | Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access. | Functional | Equal | Dedicated Privileged Account | IAC-16.4 | Mechanisms exist to assign dedicated privileged user accounts to be used solely for duties requiring privileged access. | 10 | ISM-0445 |
| ML2-P4 | Restrict administrative privileges | Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services. | Functional | Intersects With | Non-Privileged Access for Non-Security Functions | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions. | 5 | ISM-1175 |
| ML2-P4 | Restrict administrative privileges | 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. | Functional | Subset Of | Least Privilege | IAC-21 | Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions. | 10 | ISM-1175 |
| ML2-P4 | Restrict administrative privileges | Privileged users use separate privileged and unprivileged operating environments. | Functional | Intersects With | Privileged Account Management (PAM) | IAC-16 | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS). | 5 | ISM-1380 |
| ML2-P4 | Restrict administrative privileges | Privileged operating environments are not virtualised within unprivileged operating environments. | Functional | Subset Of | Privileged Environments | SEA-22 | Mechanisms exist to prevent privileged operating environments from existing within unprivileged operating environments, including physical or virtual deployments of Technology Assets, Applications and/or Services (TAAS). | 10 | ISM-1687 |
| ML2-P4 | Restrict administrative privileges | Unprivileged user accounts cannot logon to privileged operating environments. | Functional | Subset Of | Role-Based Access Control (RBAC) | IAC-08 | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with implicit business needs on Technology Assets. | 10 | ISM-1688 |
| ML2-P4 | Restrict administrative privileges | Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. | Functional | Intersects With | Non-Privileged Access for Non-Security Functions | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions. | 5 | ISM-1689 |
| ML2-P4 | Restrict administrative privileges | Administrative activities are conducted through jump servers. | Functional | Subset Of | Jump Server | AST-27 | Mechanisms exist to conduct remote system administrative functions via a "jump box" or "jump server" that is located in a separate network zone to user workstations. | 10 | ISM-1387 |
| ML2-P4 | Restrict administrative privileges | Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed. | Functional | Intersects With | Emergency Accounts | IAC-15.9 | Mechanisms exist to establish and control "emergency access only" accounts. | 8 | ISM-1685 |
| ML2-P4 | Restrict administrative privileges | Privileged access events are centrally logged. | Functional | Intersects With | Privileged Functions Logging | MON-03.3 | Mechanisms exist to log and review the actions of users and/or services with elevated privileges. | 8 | ISM-1509 |
| ML2-P4 | Restrict administrative privileges | Privileged user account and security group management events are centrally logged. | Functional | Intersects With | Privileged Functions Logging | MON-03.3 | Mechanisms exist to log and review the actions of users and/or services with elevated privileges. | 8 | ISM-1650 |
| ML2-P4 | Restrict administrative privileges | Event logs are protected from unauthorised modification and deletion. | Functional | Subset Of | Protection of Event Logs | MON-08 | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion. | 10 | ISM-1815 |
| ML2-P4 | Restrict administrative privileges | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1906 |
| ML2-P4 | Restrict administrative privileges | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1228 |
| ML2-P4 | Restrict administrative privileges | 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. | Functional | Intersects With | Event Log Analysis & Triage | MON-17 | Mechanisms exist to ensure event log reviews include analysis and triage practices that integrate with the organization's established incident response processes. | 5 | ISM-0123 |
| ML2-P4 | Restrict administrative privileges | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | Functional | Subset Of | Incident Stakeholder Reporting | IRO-10 | Mechanisms exist to timely-report incidents to applicable: 1) Internal stakeholders; 2) affected clients & third-parties; and 3) Regulatory authorities. | 10 | ISM-0140 |
| ML2-P4 | Restrict administrative privileges | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | Functional | Subset Of | Incident Handling | IRO-02 | Mechanisms exist to cover: 1) Preparation; 2) Automated event detection or manual incident report intake; 3) Analysis; 4) Containment; 5) Eradication; and 6) Recovery. | 10 | ISM-1819 |
| ML2-P5 | Application control | Application control is implemented on workstations. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 8 | ISM-0843 |
| ML2-P5 | Application control | Application control is implemented on internet-facing servers. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 5 | ISM-1490 |
| ML2-P5 | Application control | Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 5 | ISM-1870 |
| ML2-P5 | Application control | Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 5 | ISM-1871 |
| ML2-P5 | Application control | Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML, applications and control panel applets to an organisation-approved set. | Functional | Intersects With | Prevent Unauthorized Software Execution | CFG-03.2 | Mechanisms exist to configure systems to prevent the execution of unauthorized software programs. | 5 | ISM-1657 |
| ML2-P5 | Application control | Microsoft's recommended application blocklist is implemented. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1544 |
| ML2-P5 | Application control | Application control rulelets are validated on an annual or more frequent basis. | Functional | Intersects With | Reviews & Updates | CFG-02.1 | Mechanisms exist to review and update baseline configurations: 1) At least annually; 2) When required due to: so; or 3) As part of system component installations and upgrades. | 8 | ISM-1582 |
| ML2-P5 | Application control | Allowed and blocked application control events are centrally logged. | Functional | Subset Of | Content of Event Logs | MON-03 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: 1) Establish what type of event occurred; 2) When (date and time) the event occurred; 3) Where the event occurred; 4) The source of the event; 5) The outcome (success or failure) of the event; and 6) The identity of any user/subject associated with the event. | 10 | ISM-1660 |
| ML2-P5 | Application control | Event logs are protected from unauthorised modification and deletion. | Functional | Subset Of | Protection of Event Logs | MON-08 | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion. | 10 | ISM-1815 |
| ML2-P5 | Application control | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1906 |
| ML2-P5 | Application control | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1228 |
| ML2-P5 | Application control | 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. | Functional | Intersects With | Event Log Analysis & Triage | MON-17 | Mechanisms exist to ensure event log reviews include analysis and triage practices that integrate with the organization's established incident response processes. | 5 | ISM-0123 |
| ML2-P5 | Application control | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | Functional | Subset Of | Incident Stakeholder Reporting | IRO-10 | Mechanisms exist to timely-report incidents to applicable: 1) Internal stakeholders; 2) affected clients & third-parties; and 3) Regulatory authorities. | 10 | ISM-0140 |
| ML2-P5 | Application control | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | Functional | Subset Of | Incident Handling | IRO-02 | Mechanisms exist to cover: 1) Preparation; 2) Automated event detection or manual incident report intake; 3) Analysis; 4) Containment; 5) Eradication; and 6) Recovery. | 10 | ISM-1819 |
| ML2-P6 | Restrict Microsoft Office macros | Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1671 |
| ML2-P6 | Restrict Microsoft Office macros | Microsoft Office macros in files originating from the internet are blocked. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1488 |
| ML2-P6 | Restrict Microsoft Office macros | Microsoft Office macro antivirus scanning is enabled. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1672 |
| ML2-P6 | Restrict Microsoft Office macros | Microsoft Office macros are blocked from making Win32 API calls. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1673 |
| ML2-P6 | Restrict Microsoft Office macros | Microsoft Office macro security settings cannot be changed by users. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1489 |
| ML2-P7 | User application hardening | Internet Explorer 11 is disabled or removed. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1654 |
| ML2-P7 | User application hardening | Web browsers do not process Java from the internet. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1486 |
| ML2-P7 | User application hardening | Web browsers do not process web advertisements from the internet. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1485 |
| ML2-P7 | User application hardening | Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1412 |
| ML2-P7 | User application hardening | Web browser security settings cannot be changed by users. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1585 |
| ML2-P7 | User application hardening | Microsoft Office is blocked from creating child processes. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1667 |
| ML2-P7 | User application hardening | Microsoft Office is blocked from creating executable content. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1668 |
| ML2-P7 | User application hardening | Microsoft Office is blocked from injecting code into other processes. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1669 |
| ML2-P7 | User application hardening | Microsoft Office is configured to prevent activation of Object Linking and Embedding packages. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1542 |
| ML2-P7 | User application hardening | Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1859 |
| ML2-P7 | User application hardening | Office productivity suite security settings cannot be changed by users. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1823 |
| ML2-P7 | User application hardening | PDF software is blocked from creating child processes. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1670 |
| ML2-P7 | User application hardening | PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1860 |
| ML2-P7 | User application hardening | PDF software security settings cannot be changed by users. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1824 |
| ML2-P7 | User application hardening | PowerShell module logging, script block logging and transcription events are centrally logged. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1623 |
| ML2-P7 | User application hardening | Command line process creation events are centrally logged. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1889 |
| ML2-P7 | User application hardening | Event logs are protected from unauthorised modification and deletion. | Functional | Subset Of | Protection of Event Logs | MON-08 | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion. | 10 | ISM-1815 |
| ML2-P7 | User application hardening | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1906 |
| ML2-P7 | User application hardening | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1228 |
| ML2-P7 | User application hardening | 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. | Functional | Intersects With | Event Log Analysis & Triage | MON-17 | Mechanisms exist to ensure event log reviews include analysis and triage practices that integrate with the organization's established incident response processes. | 5 | ISM-0123 |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes |
|--------|-----------------------------|---|----------------|-------------------|--|-----------|---|--------------------------|----------|
| ML2-P7 | User application hardening | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | Functional | Subset Of | Incident Stakeholder Reporting | IRO-10 | Mechanisms exist to timely report incidents to applicable: (1) Internal stakeholders; (2) affected clients & third parties; and (3) Regulatory authorities. | 10 | ISM-0140 |
| ML2-P7 | User application hardening | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | Functional | Subset Of | Incident Handling | IRO-02 | Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery. | 10 | ISM-1819 |
| ML2-P8 | Regular backups | Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements. | Functional | Intersects With | Data Backups | BCD-11 | Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). | 5 | ISM-1511 |
| ML2-P8 | Regular backups | Backups of data, applications and settings are synchronized to enable restoration to a common point in time. | Functional | Intersects With | Recovery Time / Point Objectives (RTO / RPO) | BCD-01.4 | Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). | 5 | ISM-1810 |
| ML2-P8 | Regular backups | Backups of data, applications and settings are retained in a secure and resilient manner. | Functional | Intersects With | Separate Storage for Critical Information | BCD-11.2 | Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up. | 5 | ISM-1811 |
| ML2-P8 | Regular backups | Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises. | Functional | Intersects With | Test Restoration Using Sampling | BCD-11.5 | Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of business continuity plan testing. | 5 | ISM-1515 |
| ML2-P8 | Regular backups | Unprivileged user accounts cannot access backups belonging to other user accounts. | Functional | Intersects With | Backup Access | BCD-11.9 | Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations. | 5 | ISM-1812 |
| ML2-P8 | Regular backups | Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts. | Functional | Intersects With | Backup Access | BCD-11.9 | Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations. | 5 | ISM-1705 |
| ML2-P8 | Regular backups | Unprivileged user accounts are prevented from modifying and deleting backups. | Functional | Intersects With | Backup Modification and/or Destruction | BCD-11.10 | Mechanisms exist to restrict access to modify and/or delete backups to privileged users with assigned data backup and recovery operations roles. | 5 | ISM-1814 |
| ML2-P8 | Regular backups | Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups. | Functional | Intersects With | Backup Modification and/or Destruction | BCD-11.10 | Mechanisms exist to restrict access to modify and/or delete backups to privileged users with assigned data backup and recovery operations roles. | 5 | ISM-1707 |
| ML3-P1 | Patch applications | An automated method of asset discovery is used at least fortnightly to support the detection of assets for subsequent vulnerability scanning activities. | Functional | Subset Of | Asset Inventories | AST-02 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel. | 10 | ISM-1807 |
| ML3-P1 | Patch applications | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | Functional | Intersects With | Update Tool Capability | VPM-06.1 | Mechanisms exist to update vulnerability scanning tools. | 8 | ISM-1808 |
| ML3-P1 | Patch applications | A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in online services. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1658 |
| ML3-P1 | Patch applications | 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. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1699 |
| ML3-P1 | Patch applications | 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. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1700 |
| ML3-P1 | Patch applications | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1876 |
| ML3-P1 | Patch applications | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1690 |
| ML3-P1 | Patch applications | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1692 |
| ML3-P1 | Patch applications | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1901 |
| ML3-P1 | Patch applications | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1693 |
| ML3-P1 | Patch applications | Online services that are no longer supported by vendors are removed. | Functional | Subset Of | Unsupported Technology Assets, Applications and/or Services (TAAS) | TDA-17 | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs. | 10 | ISM-1905 |
| ML3-P1 | Patch applications | 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. | Functional | Subset Of | Unsupported Technology Assets, Applications and/or Services (TAAS) | TDA-17 | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs. | 10 | ISM-1704 |
| ML3-P1 | Patch applications | 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. | Functional | Subset Of | Unsupported Technology Assets, Applications and/or Services (TAAS) | TDA-17 | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs. | 10 | ISM-0304 |
| ML3-P2 | 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. | Functional | Subset Of | Asset Inventories | AST-02 | Mechanisms exist to perform inventories of Technology Assets, Applications, Services and/or Data (TAASD) that: (1) Accurately reflects the current TAASD in use; (2) Identifies authorized software products, including business justification details; (3) Is at the level of granularity deemed necessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and (5) Is available for review and audit by designated organizational personnel. | 10 | ISM-1807 |
| ML3-P2 | Patch operating systems | A vulnerability scanner with an up-to-date vulnerability database is used for vulnerability scanning activities. | Functional | Intersects With | Update Tool Capability | VPM-06.1 | Mechanisms exist to update vulnerability scanning tools. | 8 | ISM-1808 |
| ML3-P2 | Patch operating systems | 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. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1701 |
| ML3-P2 | Patch operating systems | 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. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1702 |
| ML3-P2 | Patch operating systems | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in drivers. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1703 |
| ML3-P2 | Patch operating systems | A vulnerability scanner is used at least fortnightly to identify missing patches or updates for vulnerabilities in firmware. | Functional | Intersects With | Vulnerability Scanning | VPM-06 | Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications. | 8 | ISM-1900 |
| ML3-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1877 |
| ML3-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1694 |
| ML3-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1696 |
| ML3-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1902 |
| ML3-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1879 |
| ML3-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1697 |
| ML3-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1903 |
| ML3-P2 | Patch operating systems | 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. | Functional | Subset Of | Software & Firmware Patching | VPM-05 | Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware. | 10 | ISM-1904 |
| ML3-P2 | Patch operating systems | The latest release, or the previous release, of operating systems are used. | Functional | Subset Of | Technology Lifecycle Management | SEA-07.1 | Mechanisms exist to manage the usable lifecycles of Technology Assets, Applications and/or Services (TAAS). | 10 | ISM-1407 |
| ML3-P2 | Patch operating systems | Operating systems that are no longer supported by vendors are replaced. | Functional | Subset Of | Unsupported Technology Assets, Applications and/or Services (TAAS) | TDA-17 | Mechanisms exist to prevent unsupported Technology Assets, Applications and/or Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs. | 10 | ISM-1501 |
| ML3-P3 | 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. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatable data. | 8 | ISM-1504 |
| ML3-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate users to third-party online services that process, store or communicate their organisation's sensitive data. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatable data. | 8 | ISM-1679 |
| ML3-P3 | Multi-factor authentication | 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. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatable data. | 8 | ISM-1680 |
| ML3-P3 | Multi-factor authentication | 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. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatable data. | 8 | ISM-1892 |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes |
|--------|------------------------------------|---|----------------|-------------------|--|----------|--|--------------------------|----------|
| ML3-P3 | Multi-factor authentication | 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. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1893 |
| ML3-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer data. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1681 |
| ML3-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate privileged users of systems. | Functional | Intersects With | Local Access to Privileged Accounts | IAC-06.3 | Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate local access for privileged accounts. | 8 | ISM-1173 |
| ML3-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate unprivileged users of systems. | Functional | Intersects With | Network Access to Non-Privileged Accounts | IAC-06.2 | Mechanisms exist to utilize Multi-Factor Authentication (MFA) to authenticate network access for non-privileged accounts. | 8 | ISM-0974 |
| ML3-P3 | Multi-factor authentication | Multi-factor authentication is used to authenticate users of data repositories. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1505 |
| ML3-P3 | Multi-factor authentication | Multi-factor authentication uses either: something users have and something users know, or something users have that is unlocked by something users know or see. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1401 |
| ML3-P3 | Multi-factor authentication | Multi-factor authentication used for authenticating users of online services is phishing-resistant. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1872 |
| ML3-P3 | Multi-factor authentication | Multi-factor authentication used for authenticating customers of online customer services is phishing-resistant. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1874 |
| ML3-P3 | Multi-factor authentication | Multi-factor authentication used for authenticating users of systems is phishing-resistant. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1682 |
| ML3-P3 | Multi-factor authentication | Multi-factor authentication used for authenticating users of data repositories is phishing-resistant. | Functional | Intersects With | Multi-Factor Authentication (MFA) | IAC-06 | Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulatory data. | 8 | ISM-1894 |
| ML3-P3 | Multi-factor authentication | Successful and unsuccessful multi-factor authentication events are centrally logged. | Functional | Intersects With | Content of Event Logs | MON-03 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: (1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event. | 5 | ISM-1683 |
| ML3-P3 | Multi-factor authentication | Event logs are protected from unauthorised modification and deletion. | Functional | Subset Of | Protection of Event Logs | MON-08 | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion. | 10 | ISM-1815 |
| ML3-P3 | Multi-factor authentication | Event logs from internet-facing servers are analysed in a timely manner to detect cyber security events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1906 |
| ML3-P3 | Multi-factor authentication | Event logs from non-internet-facing servers are analysed in a timely manner to detect cyber security events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1907 |
| ML3-P3 | Multi-factor authentication | Event logs from workstations are analysed in a timely manner to detect cyber security events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-0109 |
| ML3-P3 | Multi-factor authentication | Cyber security events are analysed in a timely manner to identify cyber security incidents. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1228 |
| ML3-P3 | Multi-factor authentication | Cyber security incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur or are discovered. | Functional | Intersects With | Event Log Analysis & Triage | MON-17 | Mechanisms exist to ensure event log reviews include analysis and triage practices that integrate with the organization's established incident response processes. | 5 | ISM-0123 |
| ML3-P3 | Multi-factor authentication | Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered. | Functional | Subset Of | Incident Stakeholder Reporting | IRO-10 | Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities. | 10 | ISM-0140 |
| ML3-P3 | Multi-factor authentication | Following the identification of a cyber security incident, the cyber security incident response plan is enacted. | Functional | Subset Of | Incident Handling | IRO-02 | Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery. | 10 | ISM-1819 |
| ML3-P4 | Restrict administrative privileges | Requests for privileged access to systems, applications and data repositories are validated when first requested. | Functional | Intersects With | Privileged Account Management (PAM) | IAC-16 | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS). | 5 | ISM-1507 |
| ML3-P4 | Restrict administrative privileges | Requests for privileged access to systems, applications and data repositories are validated when first requested. | Functional | Intersects With | Privileged Approval For Privileged Accounts | IAC-21.3 | Mechanisms exist to restrict the assignment of privileged accounts to management-approved personnel and/or roles. | 5 | ISM-1507 |
| ML3-P4 | Restrict administrative privileges | Privileged access to systems, applications and data repositories is disabled after 12 months unless revalidated. | Functional | Intersects With | Privileged Account Management (PAM) | IAC-16 | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS). | 3 | ISM-1647 |
| ML3-P4 | Restrict administrative privileges | Privileged access to systems and applications is disabled after 45 days of inactivity. | Functional | Intersects With | Disable Inactive Accounts | IAC-15.3 | Automated mechanisms exist to disable inactive accounts after an organization-defined time period. | 8 | ISM-1648 |
| ML3-P4 | Restrict administrative privileges | Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access. | Functional | Equal | Dedicated Privileged Account | IAC-16.4 | Mechanisms exist to assign dedicated privileged user accounts to be used solely for duties requiring privileged access. | 10 | ISM-0445 |
| ML3-P4 | Restrict administrative privileges | Privileged access to systems, applications and data repositories is limited to only what is required for users and services to undertake their duties. | Functional | Intersects With | Least Privilege | IAC-21 | Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions. | 5 | ISM-1508 |
| ML3-P4 | Restrict administrative privileges | Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet, email and web services. | Functional | Intersects With | Non-Privileged Access for Non-Security Functions | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions. | 5 | ISM-1175 |
| ML3-P4 | Restrict administrative privileges | 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. | Functional | Subset Of | Least Privilege | IAC-21 | Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions. | 10 | ISM-1883 |
| ML3-P4 | Restrict administrative privileges | Secure Admin Workstations are used in the performance of administrative activities. | Functional | Equal | Dedicated Administrative Machines | IAC-20.4 | Mechanisms exist to restrict executing administrative tasks or tasks requiring elevated access on a dedicated machine. | 10 | ISM-1898 |
| ML3-P4 | Restrict administrative privileges | Privileged users use separate privileged and unprivileged operating environments. | Functional | Intersects With | Privileged Account Management (PAM) | IAC-16 | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS). | 5 | ISM-1380 |
| ML3-P4 | Restrict administrative privileges | Privileged operating environments are not virtualised within unprivileged operating environments. | Functional | Subset Of | Privileged Environments | SEA-22 | Mechanisms exist to prevent privileged operating environments from existing within unprivileged operating environments, including physical or virtual deployments of Technology Assets, Applications and/or Services (TAAS). | 10 | ISM-1687 |
| ML3-P4 | Restrict administrative privileges | Unprivileged user accounts cannot logon to privileged operating environments. | Functional | Subset Of | Role-Based Access Control (RBAC) | IAC-08 | Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs. | 10 | ISM-1688 |
| ML3-P4 | Restrict administrative privileges | Privileged user accounts (excluding local administrator accounts) cannot logon to unprivileged operating environments. | Functional | Intersects With | Non-Privileged Access for Non-Security Functions | IAC-21.2 | Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions. | 5 | ISM-1689 |
| ML3-P4 | Restrict administrative privileges | Just-in-time administration is used for administering systems and applications. | Functional | Intersects With | Privileged Account Management (PAM) | IAC-16 | Mechanisms exist to restrict and control privileged access rights for users and Technology Assets, Applications and/or Services (TAAS). | 8 | ISM-1649 |
| ML3-P4 | Restrict administrative privileges | Administrative activities are conducted through jump servers. | Functional | Subset Of | Jump Server | AST-7 | Mechanisms exist to conduct remote system administrative functions via a 'jump box' or 'jump server' that is located in a separate network zone to user workstations. | 10 | ISM-1387 |
| ML3-P4 | Restrict administrative privileges | Credentials for break glass accounts, local administrator accounts and service accounts are long, unique, unpredictable and managed. | Functional | Intersects With | Emergency Accounts | IAC-15.9 | Mechanisms exist to establish and control 'emergency access only' accounts. | 8 | ISM-1685 |
| ML3-P4 | Restrict administrative privileges | Memory integrity functionality is enabled. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry accepted system hardening standards. | 5 | ISM-1896 |
| ML3-P4 | Restrict administrative privileges | Local Security Authority protection functionality is enabled. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry accepted system hardening standards. | 5 | ISM-1861 |
| ML3-P4 | Restrict administrative privileges | Credential Guard functionality is enabled. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry accepted system hardening standards. | 5 | ISM-1686 |
| ML3-P4 | Restrict administrative privileges | Remote Credential Guard functionality is enabled. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry accepted system hardening standards. | 5 | ISM-1897 |
| ML3-P4 | Restrict administrative privileges | Privileged access events are centrally logged. | Functional | Intersects With | Privileged Functions Logging | MON-03.3 | Mechanisms exist to log and review the actions of users and/or services with elevated privileges. | 8 | ISM-1509 |
| ML3-P4 | Restrict administrative privileges | Privileged user account and security group management events are centrally logged. | Functional | Intersects With | Privileged Functions Logging | MON-03.3 | Mechanisms exist to log and review the actions of users and/or services with elevated privileges. | 8 | ISM-1509 |
| ML3-P4 | Restrict administrative privileges | Event logs are protected from unauthorised modification and deletion. | Functional | Subset Of | Protection of Event Logs | MON-08 | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion. | 10 | ISM-1815 |
| ML3-P4 | Restrict administrative privileges | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1906 |
| ML3-P4 | Restrict administrative privileges | Event logs from non-internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1907 |
| ML3-P4 | Restrict administrative privileges | Event logs from workstations are analysed in a timely manner to detect cybersecurity events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-0109 |
| ML3-P4 | Restrict administrative privileges | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1228 |
| ML3-P4 | Restrict administrative privileges | 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. | Functional | Intersects With | Event Log Analysis & Triage | MON-17 | Mechanisms exist to ensure event log reviews include analysis and triage practices that integrate with the organization's established incident response processes. | 5 | ISM-0123 |
| ML3-P4 | Restrict administrative privileges | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | Functional | Subset Of | Incident Stakeholder Reporting | IRO-10 | Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities. | 10 | ISM-0140 |
| ML3-P4 | Restrict administrative privileges | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | Functional | Subset Of | Incident Handling | IRO-02 | Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake; (3) Analysis; (4) Containment; (5) Eradication; and (6) Recovery. | 10 | ISM-1819 |
| ML3-P5 | Application control | Application control is implemented on workstations. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 8 | ISM-0843 |
| ML3-P5 | Application control | Application control is implemented on internet-facing servers. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 8 | ISM-1490 |
| ML3-P5 | Application control | Application control is implemented on non-internet-facing servers. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 8 | ISM-1656 |
| ML3-P5 | Application control | Application control is applied to user profiles and temporary folders used by operating systems, web browsers and email clients. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 5 | ISM-1870 |
| ML3-P5 | Application control | Application control is applied to all locations other than user profiles and temporary folders used by operating systems, web browsers and email clients. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 5 | ISM-1871 |
| ML3-P5 | Application control | Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML, applications and control panel applets to an organisation-approved set. | Functional | Intersects With | Prevent Unauthorized Software Execution | CFG-03.2 | Mechanisms exist to configure systems to prevent the execution of unauthorized software programs. | 5 | ISM-1657 |
| ML3-P5 | Application control | Application control restricts the execution of drivers to an organisation-approved set. | Functional | Intersects With | Explicitly Allow / Deny Applications | CFG-03.3 | Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems. | 8 | ISM-1658 |

| FDE # | FDE Name | Focal Document Element (FDE) Description | STRM Rationale | STRM Relationship | SCF Control | SCF # | Secure Controls Framework (SCF) Control Description | Strength of Relationship | Notes |
|--------|----------------------------------|--|----------------|-------------------|--|-----------|--|--------------------------|----------|
| ML3-P5 | Application control | Microsoft's recommended application blocklist is implemented. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1544 |
| ML3-P5 | Application control | Microsoft's vulnerable driver blocklist is implemented. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1659 |
| ML3-P5 | Application control | Application control rulesets are validated on an annual or more frequent basis. | Functional | Intersects With | Reviews & Updates | CFG-02.1 | Mechanisms exist to review and update baseline configurations: 1) At least annually; 2) When required due to so; or 3) As part of system component installations and upgrades. | 8 | ISM-1582 |
| ML3-P5 | Application control | Allowed and blocked application control events are centrally logged. | Functional | Subset Of | Content of Event Logs | MON-03 | Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum: 1) Establish what type of event occurred; 2) When (date and time) the event occurred; 3) Where the event occurred; 4) The source of the event; 5) The outcome (success or failure) of the event; and 6) The identity of any user/subject associated with the event. | 10 | ISM-1660 |
| ML3-P5 | Application control | Event logs are protected from unauthorised modification and deletion. | Functional | Subset Of | Protection of Event Logs | MON-08 | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion. | 10 | ISM-1815 |
| ML3-P5 | Application control | Event logs from non-internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1906 |
| ML3-P5 | Application control | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1907 |
| ML3-P5 | Application control | Event logs from workstations are analysed in a timely manner to detect cybersecurity events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-0109 |
| ML3-P5 | Application control | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1228 |
| ML3-P5 | Application control | 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. | Functional | Intersects With | Event Log Analysis & Triage | MON-17 | Mechanisms exist to ensure event log reviews include analysis and triage practices that integrate with the organization's established incident response processes. | 5 | ISM-0123 |
| ML3-P5 | Application control | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | Functional | Subset Of | Incident Stakeholder Reporting | IRO-10 | Mechanisms exist to timely-report incidents to applicable: 1) Internal stakeholders; 2) Affected clients & third parties; and 3) Regulatory authorities. | 10 | ISM-0140 |
| ML3-P5 | Application control | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | Functional | Subset Of | Incident Handling | IRO-02 | Mechanisms exist to cover: 1) Preparation; 2) Automated event detection or manual incident report intake; 3) Analysis; 4) Containment; 5) Eradication; and 6) Recovery. | 10 | ISM-1819 |
| ML3-P6 | Restrict Microsoft Office macros | Microsoft Office macros are disabled for users that do not have a demonstrated business requirement. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1671 |
| ML3-P6 | Restrict Microsoft Office macros | 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. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1674 |
| ML3-P6 | Restrict Microsoft Office macros | Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted Locations. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1890 |
| ML3-P6 | Restrict Microsoft Office macros | Only privileged users responsible for checking that Microsoft Office macros are free of malicious code can write to and modify content within Trusted Locations. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1487 |
| ML3-P6 | Restrict Microsoft Office macros | Microsoft Office macros digitally signed by an untrusted publisher cannot be enabled via the Message Bar or Backstage View. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1675 |
| ML3-P6 | Restrict Microsoft Office macros | Microsoft Office macros digitally signed by signatures other than V3 signatures cannot be enabled via the Message Bar or Backstage View. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1891 |
| ML3-P6 | Restrict Microsoft Office macros | Microsoft Office's list of trusted publishers is validated on an annual or more frequent basis. | Functional | Intersects With | Reviews & Updates | CFG-02.1 | Mechanisms exist to review and update baseline configurations: 1) At least annually; 2) When required due to so; or 3) As part of system component installations and upgrades. | 5 | ISM-1676 |
| ML3-P6 | Restrict Microsoft Office macros | Microsoft Office macros in files originating from the internet are blocked. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1488 |
| ML3-P6 | Restrict Microsoft Office macros | Microsoft Office macro antivirus scanning is enabled. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1672 |
| ML3-P6 | Restrict Microsoft Office macros | Microsoft Office macros are blocked from making Win32 API calls. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1673 |
| ML3-P6 | Restrict Microsoft Office macros | Microsoft Office macro security settings cannot be changed by users. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1489 |
| ML3-P7 | User application hardening | Internet Explorer 11 is disabled or removed. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1654 |
| ML3-P7 | User application hardening | Web browsers do not process Java from the internet. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1486 |
| ML3-P7 | User application hardening | Web browsers do not process web advertisements from the internet. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1485 |
| ML3-P7 | User application hardening | Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1412 |
| ML3-P7 | User application hardening | Web browser security settings cannot be changed by users. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1585 |
| ML3-P7 | User application hardening | Microsoft Office is blocked from creating child processes. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1667 |
| ML3-P7 | User application hardening | Microsoft Office is blocked from creating executable content. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1668 |
| ML3-P7 | User application hardening | Microsoft Office is blocked from injecting code into other processes. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1669 |
| ML3-P7 | User application hardening | Microsoft Office is configured to prevent activation of Object Linking and Embedding packages. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1542 |
| ML3-P7 | User application hardening | Office productivity suites are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1859 |
| ML3-P7 | User application hardening | Office productivity suite security settings cannot be changed by users. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1823 |
| ML3-P7 | User application hardening | PDF software is blocked from creating child processes. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1670 |
| ML3-P7 | User application hardening | PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts occur. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1860 |
| ML3-P7 | User application hardening | PDF software security settings cannot be changed by users. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1824 |
| ML3-P7 | User application hardening | .NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1655 |
| ML3-P7 | User application hardening | Windows PowerShell 2.0 is disabled or removed. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1621 |
| ML3-P7 | User application hardening | PowerShell is configured to use Constrained Language Mode. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1622 |
| ML3-P7 | User application hardening | PowerShell module logging, script block logging and transcription events are centrally logged. | Functional | Intersects With | Secure Baseline Configurations | CFG-02 | Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. | 5 | ISM-1623 |
| ML3-P7 | User application hardening | Command line process creation events are centrally logged. | Functional | Intersects With | Privileged Functions Logging | MON-03.3 | Mechanisms exist to log and review the actions of users and/or services with elevated privileges. | 5 | ISM-1889 |
| ML3-P7 | User application hardening | Event logs are protected from unauthorised modification and deletion. | Functional | Subset Of | Protection of Event Logs | MON-08 | Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion. | 10 | ISM-1815 |
| ML3-P7 | User application hardening | Event logs from non-internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1906 |
| ML3-P7 | User application hardening | Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1907 |
| ML3-P7 | User application hardening | Event logs from workstations are analysed in a timely manner to detect cybersecurity events. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-0109 |
| ML3-P7 | User application hardening | Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents. | Functional | Intersects With | Central Review & Analysis | MON-02.2 | Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. | 5 | ISM-1228 |
| ML3-P7 | User application hardening | 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. | Functional | Intersects With | Event Log Analysis & Triage | MON-17 | Mechanisms exist to ensure event log reviews include analysis and triage practices that integrate with the organization's established incident response processes. | 5 | ISM-0123 |
| ML3-P7 | User application hardening | Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered. | Functional | Subset Of | Incident Stakeholder Reporting | IRO-10 | Mechanisms exist to timely-report incidents to applicable: 1) Internal stakeholders; 2) Affected clients & third parties; and 3) Regulatory authorities. | 10 | ISM-0140 |
| ML3-P7 | User application hardening | Following the identification of a cybersecurity incident, the cybersecurity incident response plan is enacted. | Functional | Subset Of | Incident Handling | IRO-02 | Mechanisms exist to cover: 1) Preparation; 2) Automated event detection or manual incident report intake; 3) Analysis; 4) Containment; 5) Eradication; and 6) Recovery. | 10 | ISM-1819 |
| ML3-P8 | Regular backups | Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity requirements. | Functional | Intersects With | Data Backups | BCD-11 | Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfy Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). | 5 | ISM-1511 |
| ML3-P8 | Regular backups | Backups of data, applications and settings are synchronized to enable restoration to a common point in time. | Functional | Intersects With | Recovery Time / Point Objectives (RTO / RPO) | BCD-01.4 | Mechanisms exist to facilitate recovery operations in accordance with Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). | 5 | ISM-1810 |
| ML3-P8 | Regular backups | Backups of data, applications and settings are retained in a secure and resilient manner. | Functional | Intersects With | Separate Storage for Critical Information | BCD-11.2 | Mechanisms exist to store backup copies of critical software and other security-related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up. | 5 | ISM-1811 |
| ML3-P8 | Regular backups | Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises. | Functional | Intersects With | Test Restoration Using Sampling | BCD-11.5 | Mechanisms exist to utilize sampling of available backups to test recovery capabilities as part of system continuity plan testing. | 5 | ISM-1515 |
| ML3-P8 | Regular backups | Unprivileged user accounts cannot access backups belonging to other user accounts. | Functional | Intersects With | Backup Access | BCD-11.9 | Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations. | 5 | ISM-1812 |
| ML3-P8 | Regular backups | Unprivileged user accounts cannot access their own backups. | Functional | Intersects With | Backup Access | BCD-11.9 | Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations. | 5 | ISM-1813 |
| ML3-P8 | Regular backups | Privileged user accounts (excluding backup administrator accounts) cannot access backups belonging to other user accounts. | Functional | Intersects With | Backup Access | BCD-11.9 | Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations. | 5 | ISM-1705 |
| ML3-P8 | Regular backups | Privileged user accounts (excluding backup administrator accounts) cannot access their own backups. | Functional | Intersects With | Backup Access | BCD-11.9 | Mechanisms exist to restrict access to backups to privileged users with assigned roles for data backup and recovery operations. | 5 | ISM-1706 |
| ML3-P8 | Regular backups | Unprivileged user accounts are prevented from modifying and deleting backups. | Functional | Intersects With | Backup Modification and/or Destruction | BCD-11.10 | Mechanisms exist to restrict access to modify and/or delete backups to privileged users with assigned data backup and recovery operations roles. | 5 | ISM-1814 |
| ML3-P8 | Regular backups | Privileged user accounts (excluding backup administrator accounts) are prevented from modifying and deleting backups. | Functional | Intersects With | Backup Modification and/or Destruction | BCD-11.10 | Mechanisms exist to restrict access to modify and/or delete backups to privileged users with assigned data backup and recovery operations roles. | 5 | ISM-1707 |
| ML3-P8 | Regular backups | Backup administrator accounts are prevented from modifying and deleting backups during their retention period. | Functional | Intersects With | Backup Modification and/or Destruction | BCD-11.10 | Mechanisms exist to restrict access to modify and/or delete backups to privileged users with assigned data backup and recovery operations roles. | 5 | ISM-1708 |