NISTIR 8477-Based Set Theory Relationship Mapping (STRM)
Reference Document: Secure Controls Framework (SCF) version 2025.3
STRM Guldance: https://securecontrolsframework.com/set-theory-relationship-mapping-strm/

lished STRM URL:	https://securecontrols framework.com/content/strm/scf-strm-apac-australia-essential-8.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 (optional)	Notes (optional)
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 (TASD) that: (1) Accurately reflects the current TASD in use; (2) Identifies authorized software products, including business justification details (3) lat 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 sudit 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) [1]; (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, wendor or manufacturer, and [2] Requiring justification and documented approval for the continued use of unsupported TAAS required to astitute, mission/flustingss 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) [1]; (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, wendor or manufacturer, and [2] Requiring justification and documented approval for the continued use of unsupported TAAS required to astitute, mission/flustiness 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 properly 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	A vulnerability scanner is used at least daily to identify missing patches or updates for vulnerabilities in operating systems of internet-facing	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	servers and internet-facing network devices. 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	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	network devices. 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	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	exploits exist. 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 workers and no working	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	exploits exist. 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	Hechnalisms exist to prevent unsupported Technology Assets, Applications and/or Sencies (TAAS) pr; (1) Removing and/or replacing TAAS when support for the components is no longer available from the developer, wendor or manufacturer, and 2) Requiring justification and documented approval for the continued use of unsupported TAAS required to astity, mission/flusiness 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/regulated 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) Intir-party Fenhology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated 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) Tindr-party Fenhology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated 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) Tindr-party Fethonology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated 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) Timid-party Fethonology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated 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) Timic party Fethology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	8	ISM-1681
ML1-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) Tinid-party Fethology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated 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

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
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 duties requiring privileged access.	10	ISM-0445
ML1-P4	Restrict administrative	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet,	Functional	Intersects With	Non-Privileged Access for	IAC-21.2	Mechanisms exist to prohibit privileged users from using privileged accounts, while performing non-security functions.	5	ISM-1175
	privileges	email and web services. Privileged user accounts explicitly authorised to access online services			Non-Security Functions		Mechanisms exist to utilize the concept of least privilege, allowing only authorized		ISM-1883
ML1-P4	Restrict administrative privileges	are strictly limited to only what is required for users and services to undertake their duties.	Functional	Subset Of	Least Privilege	IAC-21	access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	10	
ML1-P4	Restrict administrative privileges	undertake their dudes. Privileged users use separate privileged and unprivileged operating environments.	Functional	Intersects With	Privileged Account	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and	5	ISM-1380
	Restrict administrative	Unprivileged user accounts cannot logon to privileged operating			Management (PAM) Role-Based Access		Technology Assets, Applications and/or Services (TAAS). Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology		ISM-1688
ML1-P4	privileges	environments.	Functional	Subset Of	Control (RBAC)	IAC-08	Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs.	10	
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	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist /	8	ISM-0843
ML1-P5	Application control	Application control is applied to user profiles and temporary folders	Functional	Intersects With	Applications Explicitly Allow / Deny	CFG-03.3	blacklist) applications that are authorized to execute on systems. Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist /	5	ISM-1870
		used by operating systems, web browsers and email clients. Application control restricts the execution of executables, software			Applications Explicitly Allow / Deny		blacklist) applications that are authorized to execute on systems. Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist /		ISM-1657
ML1-P5	Application control	libraries, scripts, installers, compiled HTML, HTML applications and control panel applets to an organisation-approved set.	Functional	Intersects With	Applications	CFG-03.3	blacklist) applications that are authorized to execute on systems.	5	
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	5	ISM-1671
	Restrict Microsoft	·			=		consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline		ISM-1488
ML1-P6	Office macros	Microsoft Office macros in files originating from the internet are blocked.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
ML1-P6	Restrict Microsoft	Microsoft Office macro antivirus scanning is enabled.	Functional	Intersects With	Secure Baseline	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1672
	Office macros				Configurations		consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline		ISM-1489
ML1-P6	Restrict Microsoft Office macros	Microsoft Office macro security settings cannot be changed by users.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	1405
ML1-P7	User application	Internet Explorer 11 is disabled or removed.	Functional	Intersects With	Secure Baseline	CFG-02	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets. Applications and/or Services (TAAS) that are	5	ISM-1654
PILI-P/	hardening	Internet explorer i i is disabled or removed.	runctionat	intersects with	Configurations	CFG-02	consistent with industry-accepted system hardening standards.	5	
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	5	ISM-1486
	User application				Secure Baseline		consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline		ISM-1485
ML1-P7	hardening	Web browsers do not process web advertisements from the internet.	Functional	Intersects With	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
ML1-P7	User application	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	5	ISM-1585
	hardening				Configurations		consistent with industry-accepted system hardening standards. Mechanisms exist to create recurring backups of data, software and/or system		ISM-1511
ML1-P8	Regular backups	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity	Functional	Intersects With	Data Backups	BCD-11	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	5	
		requirements. Backups of data, applications and settings are synchronised to enable			Recovery Time / Point		(RPOs). Mechanisms exist to facilitate recovery operations in accordance with Recovery		ISM-1810
ML1-P8	Regular backups	restoration to a common point in time.	Functional	Intersects With	Objectives (RTO / RPO)	BCD-01.4	Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	ISM-1811
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	5	131-1611
		Restoration of data, applications and settings from backups to a			Test Restoration Using		collocated with the system being backed up. Mechanisms exist to utilize sampling of available backups to test recovery		ISM-1515
ML1-P8	Regular backups	common point in time is tested as part of disaster recovery exercises.	Functional	Intersects With	Sampling	BCD-11.5	7,1	5	
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	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 fornightly to support the detection of assets for subsequent vulnerability scanning activities.	Functional	Subset Of	Asset Inventories	AST-02	Mechanism exist to perform inventories of Technology Assets, Applications, Services and/or Data (TASD) hat: (1) Accurately reflects the current TASD in use; (2) identifies authorized software products, including business justification details; (3) is at the level of granularity deemed raccessary for tracking and reporting; (4) Includes organization-defined information deemed necessary to achieve effective property accountability; and produced in the control of	10	ISM-1807
							(5) Is available for review and audit by designated organizational personnel.		
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
		A vulnerability scanner is used at least weekly to identify missing patches or updates for vulnerabilities in office productivity suites, web					Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.		ISM-1699
ML2-P1	Patch applications	browsers and their extensions, email clients, PDF software, and security products.	Functional	Intersects With	Vulnerability Scanning	VPM-06		8	
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
MI = 5-	Date to a series of	Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within 48 hours of release when	Power!	0.4.	Software & Firmware	V/D1:	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.		ISM-1876
ML2-P1	Patch applications	vulnerabilities are assessed as critical by vendors or when working exploits exist.	Functional	Subset Of	Patching	VPM-05		10	
		Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when	_	_	Software & Firmware		Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.		ISM-1690
ML2-P1	Patch applications	vulnerabilities are assessed as non-critical by vendors and no working exploits exist.	Functional	Subset Of	Patching	VPM-05	, solding introduction	10	
		exploits exist. Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web browsers and their extensions, email			Software & Firmware		Mechanisms exist to conduct software patching for all deployed Technology		ISM-1691
ML2-P1	Patch applications	clients, PDF software, and security products are applied within two	Functional	Subset Of	Patching	VPM-05	Assets, Applications and/or Services (TAAS), including firmware.	10	
		weeks of release. Patches, updates or other vendor mitigations for vulnerabilities in			C-4		Mechanisms exist to conduct software patching for all deployed Technology		ISM-1693
ML2-P1	Patch applications	applications other than office productivity suites, web browsers and their extensions, email clients, PDF software, and security products	Functional	Subset Of	Software & Firmware Patching	VPM-05	Assets, Applications and/or Services (TAAS), including firmware.	10	
—	1	are applied within one month of release.					Mechanisms exist to prevent unsupported Technology Assets, Applications and/or	 	ISM-1905
ML2-P1	Patch applications	Callanda	Functional	Subset Of	Unsupported Technology	TDA-17	Services (TAAS) by: (1) Removing and/or replacing TAAS when support for the components is no longer	10	
ML2-P1	Patch applications	Online services that are no longer supported by vendors are removed.	Functional	Subset Of	Assets, Applications and/or Services (TAAS)	IDA-17	available from the developer, vendor or manufacturer; and (2) Requiring justification and documented approval for the continued use of	10	
							unsupported TAAS required to satisfy mission/business needs. Mechanisms exist to prevent unsupported Technology Assets, Applications and/or		ISM-1704
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	Services (TAAS) by: If) 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 obcumented approval for the continued use of unsupported TAAS required to attiff mission/business needs. Mechanism askits to perform inventions of Technology Assets, Applications,	10	ISM-1807
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	Services and/or Data (IAASD) that: (1) Accurately reflects the current IAASD in use; (2) Identifies authorized ontware products, including business justification details; (3) is at the level of granularly 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	
ML2-P2	Patch operating	A vulnerability scanner with an up-to-date vulnerability database is	Functional	Intersects With	Update Tool Capability	VPM-06.1	Mechanisms exist to update vulnerability scanning tools.	8	ISM-1808
	systems Patch operating	used for vulnerability scanning activities. A vulnerability scanner is used at least daily to identify missing patches	Port 12 1	later 1 1111	Midney 22 6	1,000	Mechanisms exist to detect vulnerabilities and configuration errors by routine	_	ISM-1701
ML2-P2	systems	or updates for vulnerabilities in operating systems of internet-facing servers and internet-facing network devices.	Functional	Intersects With	Vulnerability Scanning	VPM-06	vulnerability scanning of systems and applications.	8	ISM 1702
ML2-P2	Patch operating systems	A vulnerability scanner is used at least fornightly 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



Secure Controls Framework (SCF) 2 of

FDE#	FDE Name	Focal Document Element (FDE) Description	STRM	STRM	SCF Control	SCF#	Secure Controls Framework (SCF)	Strength of Relationship	Notes (optional)
		Patches, updates or other vendor mitigations for vulnerabilities in	Rationale	Relationship			Control Description Mechanisms exist to conduct software patching for all deployed Technology	(optional)	ISM-1877
ML2-P2	Patch operating systems	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	Assets, Applications and/or Services (TAAS), including firmware.	10	
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 two weeks of release when vulnerabilities are assessed as non-critical by vendors and no working exoloits wast.	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: If Removing and/or replacing TAAS when support for the components is no longer available from the developer, vendor or manufacturer; and [2] Requiring Lifetiation and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs. Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:	10	ISM-1501
ML2-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 emborce Hutta-Factor Authentication (PMA) for: If 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/regulated data.	8	ISM-15U4
ML2-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) Timid-party Fethology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated 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 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/regulated data.	8	ISM-1680
ML2-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/regulated 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 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) Tilrid-party Fehnology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated 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/regulated 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	8	ISM-0974
ML2-P3	Multi-factor authentication	or systems. 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	network access for non-privileged accounts. Automated mechanisms exist to enforce Multi-factor Authentication (MFA) for: (1) Remote network access; (2) Third-party Fechnology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated 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 Fehnology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	8	ISM-1872
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) Timid-party Fethology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated 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) Timid-party Fethology Assets, Applications and/or Services (TAAS); and/ or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated 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 Assist, 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) When the event occurred; (4) The source of the event; (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 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-P3	Multi-factor authentication	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-P3	Multi-factor authentication	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-P3	Multi-factor authentication	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-P3	Multi-factor authentication	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) Endication; 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		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 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	Privileged users are assigned a dedicated privileged user account to be	Functional	Equal	Dedicated Privileged	IAC-16.4	Mechanisms exist to assign dedicated privileged user accounts to be used solely	10	ISM-0445
	privileges	used solely for duties requiring privileged access.		-4-4	Account	0.4	for duties requiring privileged access.		I



ecure Controls Framework (SCF)

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 (optional)
ML2-P4	Restrict administrative privileges	Privileged user accounts (excluding those explicitly authorised to access online services) are prevented from accessing the internet,	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	email and web services. Privileged user accounts explicitly authorised to access online services are strictly limited to only what is required for users and services to	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	10	ISM-1883
ML2-P4	privileges Restrict administrative	undertake their duties. Privileged users use separate privileged and unprivileged operating	Functional	Intersects With	Privileged Account	IAC-16	organizational business functions. Mechanisms exist to restrict and control privileged access rights for users and	5	ISM-1380
ML2-P4		environments. Privileged operating environments are not virtualised within	Functional	Subset Of	Management (PAM) Privileged Environments	SEA-22	Technology Assets, Applications and/or Services (TAAS). Mechanisms exist to prevent privileged operating environments from existing within unprivileged operating environments, including physical or virtual	10	ISM-1687
	privileges Restrict administrative	unprivileged operating environments. Unprivileged user accounts cannot logon to privileged operating			Role-Based Access		deployments of Technology Assets, Applications and/or Services (TAAS). Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology		ISM-1688
ML2-P4	privileges	environments.	Functional	Subset Of	Control (RBAC)	IAC-08	Assets, Applications, Services and/or Data (TAASD) to restrict access to individuals assigned specific roles with legitimate business needs. Mechanisms exist to prohibit privileged users from using privileged accounts,	10	ISM-1689
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	white performing non-security functions.	5	
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	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	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. Cybersecurity incidents are reported to the chief information security	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 ISM-0123
ML2-P4	Restrict administrative privileges	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	1541-0123
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	10	ISM-0140
	privitages	they occur or are discovered.			Reporting		(2) Anecedo ciente & unito-parties; and (3) Regulatory authorities. Mechanisms exist to cover:		ISM-1819
	Postriat administrativa	Following the identification of a cybersecurity incident, the					(1) Preparation; (2) Automated event detection or manual incident report intake;		
ML2-P4	privileges	cybersecurity incident response plan is enacted.	Functional	Subset Of	Incident Handling	IRO-02	(3) Analysis; (4) Containment;	10	
					Explicitly Allow / Deny		(5) Eradication; and (6) Recovery Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist /		ISM-0843
ML2-P5	Application control	Application control is implemented on workstations.	Functional	Intersects With	Applications Explicitly Allow / Deny	CFG-03.3	blacklist) applications that are authorized to execute on systems. Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist /	8	ISM-1490
ML2-P5	Application control	Application control is implemented on internet-facing servers. Application control is applied to user profiles and temporary folders	Functional	Intersects With	Applications Explicitly Allow / Deny	CFG-03.3	blacklist) applications that are authorized to execute on systems. Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist /	5	ISM-1870
ML2-P5	Application control	used by operating systems, web browsers and email clients. Application control is applied to all locations other than user profiles	Functional	Intersects With	Applications	CFG-03.3	blacklist) applications that are authorized to execute on systems. Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist /	5	ISM-1871
ML2-P5	Application control	and temporary folders used by operating systems, web browsers and email clients.	Functional	Intersects With	Explicitly Allow / Deny Applications	CFG-03.3	blacklist) applications that are authorized to execute on systems.	5	
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	5	ISM-1544
		Application control rulesets are validated on an annual or more			-		consistent with industry-accepted system hardening standards. Mechanisms exist to review and update baseline configurations: (1) At least annually;		ISM-1582
ML2-P5	Application control	frequent basis.	Functional	Intersects With	Reviews & Updates	CFG-02.1	(2) When required due to so; or (3) As part of system component installations and upgrades.	8	
							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:		ISM-1660
ML2-P5	Application control	Allowed and blocked application control events are centrally logged.	Functional	Subset Of	Content of Event Logs	MON-03	(3) Where the event occurred; (4) The source of the event;	10	
							(5) The outcome (success or failure) of the event; and (6) The identity of any user/subject associated with the event.		
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	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
		or are discovered. Cybersecurity incidents are reported to ASD as soon as possible after			Incident Stakeholder		Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders;		ISM-0140
ML2-P5	Application control	they occur or are discovered.	Functional	Subset Of	Reporting	IRO-10	(2) Affected clients & third-parties; and (3) Regulatory authorities.	10	
							Mechanisms exist to cover: (1) Preparation; (2) Automated event detection or manual incident report intake:		ISM-1819
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	(2) Analysis; (4) Containment;	10	
							(5) Eradication; and (6) Recovery.		
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	5	ISM-1488
ML2-P6	Restrict Microsoft	Microsoft Office macro antivirus scanning is enabled.	Functional	Intersects With	Secure Baseline	CFG-02	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1672
	Office macros Restrict Microsoft				Configurations Secure Baseline		consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline		ISM-1673
ML2-P6	Office macros	Microsoft Office macros are blocked from making Win32 API calls.	Functional	Intersects With	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	5	ISM-1489
ML2-P6	Restrict Microsoft Office macros	Microsoft Office macro security settings cannot be changed by users.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
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	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	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1485
ML2-P7	User application	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when	Functional	Intersects With	Secure Baseline	CFG-02	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1412
	hardening User application	conflicts occur.			Configurations Secure Baseline		consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline		ISM-1585
ML2-P7	hardening	Web browser security settings cannot be changed by users.	Functional	Intersects With	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	5	ISM-1667
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	
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	5	ISM-1668
ML2-P7	User application	Microsoft Office is blocked from injecting code into other processes.	Functional	Intersects With	Secure Baseline	CFG-02	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1669
	hardening			1	Configurations		consistent with industry-accepted system hardening standards.	l	



ecure Controls Framework (SCF) 4 of 9

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 (optional)
	User application	Microsoft Office is configured to prevent activation of Object Linking			Secure Baseline		Mechanisms exist to develop, document and maintain secure baseline	(optional)	ISM-1542
ML2-P7	hardening	and Embedding packages. Office productivity suites are hardened using ASD and vendor	Functional	Intersects With	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	5	ISM-1859
ML2-P7	User application hardening	hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
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	5	ISM-1670
ML2-P7	User application	PDF software is hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when conflicts	Functional	Intersects With	Secure Baseline	CFG-02	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1860
ML2-P7	hardening User application	occur. PDF software security settings cannot be changed by users.	Functional	Intersects With	Configurations Secure Baseline	CFG-02	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1824
ML2-F7	hardening User application	PowerShell module logging, script block logging and transcription	runcuonat		Configurations Secure Baseline	C10-02	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline		ISM-1623
ML2-P7	hardening	events are centrally logged.	Functional	Intersects With	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	5	ISM-1889
ML2-P7	User application hardening	Command line process creation events are centrally logged.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
ML2-P7	User application hardening	Event logs are protected from unauthorised modification and deletion.	Functional	Subset Of	Protection of Event Logs Central Review &	MON-08	Mechanisms exist to protect event logs and audit tools from unauthorized access, modification and deletion.	10	ISM-1815 ISM-1906
ML2-P7	User application hardening User application	Event logs from internet-facing servers are analysed in a timely manner to detect cybersecurity events. Cybersecurity events are analysed in a timely manner to identify	Functional	Intersects With	Analysis Central Review &	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. Automated mechanisms exist to centrally collect, review and analyze audit	5	ISM-1228
ML2-P7	hardening	cybersecurity incidents.	Functional	Intersects With	Analysis	MON-02.2	records from multiple sources.	5	
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
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
							Mechanisms exist to cover: (1) Preparation:		ISM-1819
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	(2) Automated event detection or manual incident report intake; (3) Analysis;	10	
	maraching	cybridectiny modern response paints ensered.					(4) Containment; (5) Eradication; and (6) Recovery.		
ML2-P8	Regular backups	Backups of data, applications and settings are performed and retained in accordance with business criticality and business continuity	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	5	ISM-1511
		requirements. Backups of data, applications and settings are synchronised to enable			Recovery Time / Point		the data to satisfy Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Mechanisms exist to facilitate recovery operations in accordance with Recovery		ISM-1810
ML2-P8	Regular backups	restoration to a common point in time. Backups of data, applications and settings are retained in a secure and	Functional	Intersects With	Objectives (RTO / RPO) Separate Storage for	BCD-01.4	Time Objectives (RTOs) and Recovery Point Objectives (RPOs). Mechanisms exist to store backup copies of critical software and other security-	5	ISM-1811
ML2-P8	Regular backups	resilient manner.	Functional	Intersects With	Critical Information	BCD-11.2	related information in a separate facility or in a fire-rated container that is not collocated with the system being backed up. Mechanisms exist to utilize sampling of available backups to test recovery	5	ISM-1515
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	capabilities as part of business continuity plan testing.	5	1311-1313
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. Mechanisms exist to restrict access to backups to privileged users with assigned	5	ISM-1705
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	roles for data backup and recovery operations.	5	
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 fornightly 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 (flASD) hat: (1) Accurately reflects the current TAASD in use; (2) identifies authorized software products, including business justification details; (3) is at the level of granularly 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-1698
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,	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	PDF software, and security products. 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	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	exploits exist. Patches, updates or other vendor mitigations for vulnerabilities in online services are applied within two weeks of release when	Functional	Subset Of	Software & Firmware	VPM-05	Mechanisms exist to conduct software patching for all deployed Technology Assets, Applications and/or Services (TAAS), including firmware.	10	ISM-1690
		vulnerabilities are assessed as non-critical by vendors and no working exploits exist. Patches, updates or other vendor mitigations for vulnerabilities in			Patching	05	Mechanisms exist to conduct software patching for all deployed Technology	-	ISM-1692
ML3-P1	Patch applications	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	Assets, Applications and/or Services (TAAS), including firmware.	10	
ML3-P1	Patch applications	Patches, update so other working exputs east. Patches, updates or other vendor mitigations for vulnerabilities in office productivity suites, web prowsers 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	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	vendors and no working exploits exist. 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	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
		are applied within one month of release.					Mechanisms exist to prevent unsupported Technology Assets, Applications and/or		ISM-1905
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	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 TAS required to safety mission/business needs.	10	
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 (TASS) 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 lustflication and documented approval for the continued use of	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	unsupported TASS required to attain mission/business needs. Mechanism exists to prevent unsupported Technology Assets, Applications and/or Services (TAS) by: 1) Removing and/or replacing TASS when support for the components is no longer availables from the developer, wendor or manufacturer; and 2) Requiring justification and documented approval for the continued use of	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	unsupported TAAS required to statish mission/business needs. Mechanism exists perform inventione of Technology Assets, Applications, Sarvices 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 organizations] personnel.	10	ISM-1807



ecure Controls Framework (SCF) 5 o

Margins	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 (optional)
March Marc	More	Patch operating	A vulnerability scanner with an up-to-date vulnerability database is			Lindata T10	V/DM CT		(optional)	ISM-1808
The color			used for vulnerability scanning activities. A vulnerability scanner is used at least daily to identify missing patches					Mechanisms exist to detect vulnerabilities and configuration errors by routine		ISM-1701
March Marc	ML3-P2			Functional	Intersects With	Vulnerability Scanning	VPM-06	vulnerability scanning of systems and applications.	8	
March Marc	MI 2 D2	Patch operating		Eupational	Interports With	Vulnerability Seepping	VDM OF			ISM-1702
March Marc	PIESTEZ	· ·	network devices.	runctionat	III tersects with	vutilerability 3canning	VF1-1-00			
March Marc	ML3-P2		patches or updates for vulnerabilities in drivers.	Functional	Intersects With	Vulnerability Scanning	VPM-06	vulnerability scanning of systems and applications.	8	
March Marc	ML3-P2		patches or updates for vulnerabilities in firmware.	Functional	Intersects With	Vulnerability Scanning	VPM-06		8	
Part		Datab assessing				C-4 0 Fi		Mechanisms exist to conduct software patching for all deployed Technology		ISM-1877
Property	ML3-P2			Functional	Subset Of		VPM-05		10	
A								Mechanisms exist to conduct software patching for all deployed Technology		ISM-1694
March Marc	ML3-P2			Functional	Subset Of		VPM-05	Assets, Applications and/or Services (TAAS), including firmware.	10	
Prof. Prof		systems				Patching				
Process Proc		Datab assessing				C-4 0 Fi				ISM-1696
March Process Proces	ML3-P2			Functional	Subset Of		VPM-05		10	
March Marc								Mechanisms exist to conduct software patching for all deployed Technology		ISM-1902
Public Column Public Colum	ML3-P2			Functional	Subset Of		VPM-05	Assets, Applications and/or Services (TAAS), including firmware.	10	
March 1987		systems				Patching				
March Marc	ML3-P2		Patches, updates or other vendor mitigations for vulnerabilities in	Functional	Subset Of		VPM-05		10	ISM-1879
March Control Contro		systems				Patening		Mechanisms exist to conduct software patching for all deployed Technology		ISM-1697
March Common Continue of C	ML3-P2		drivers are applied within one month of release when vulnerabilities are	Functional	Subset Of		VPM-05		10	
Part			Patches, updates or other vendor mitigations for vulnerabilities in			Software & Eir		Mechanisms exist to conduct software patching for all deployed Technology		ISM-1903
March Marc	ML3-P2		firmware are applied within 48 hours of release when vulnerabilities are	Functional	Subset Of		VPM-05	Assets, Applications and/or Services (TAAS), including firmware.	10	
Month Continue Property Property of the state of the property of the property of the state of the property of the state of the property of the	MI 3-D3			Functional	Subset Of		VPM-0F		10	ISM-1904
March Marc	PILOTPZ		are assessed as non-critical by vendors and no working exploits exist.	. a.retiofiat	CADSEL UI	Patching	***************************************		10	
Mail Section Continues Processing Section	ML3-P2		The latest release, or the previous release, of operating systems are used.	Functional	Subset Of		SEA-07.1	Mechanisms exist to manage the usable lifecycles of technology assets.	10	ISM-1407
March Control Contro						ll				ISM-1501
Half-control state of the control of	ML3-P2			Functional	Subset Of	Assets, Applications	TDA-17		10	
Mail Force						and/or services (TAAS)		(2) Requiring justification and documented approval for the continued use of unsupported TAAS required to satisfy mission/business needs.		
Higher Mathematical Proposedors of the proposedors								Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:		ISM-1504
Hall Section and the expension of the control of th	ML3-P3			Functional	Intersects With		IAC-06		8	
High Part of the Committee of the Commit		authentication	their organisation's sensitive data.			Authentication (MFA)		sensitive/regulated data.		
HS-77 Mil-Stollar								Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:		ISM-1679
Militario del processo del constitución del constitución del processo del pr			Multi-factor authentication is used to authenticate users to third-party							
Half-factor authentication where preliated in solid to authenticate to where department of the communication and the operation of the communication and the communication and the operation of the communication and the communicati	ML3-P3			Functional	Intersects With		IAC-06		8	
Half-factor authentication where preliated in solid to authenticate to where department of the communication and the operation of the communication and the communication and the operation of the communication and the communicati										
MIL-179 Professional control to this big days on points exvices that process, on process on the process, the or communicate annual form of the process. The process of the								(1) Remote network access;		ISM-1680
Mail Factor authentication is used to authentication authenticatio	ML3-P3		users to third-party online services that process, store or	Functional	Intersects With		IAC-06		8	
Multi-Sector understandard was also all consideration with seal to authentication was a facility of the section of the continue of the continu		authentication	communicate their organisation's non-sensitive data.			Authentication (MPA)				
Mill-Parties Mill-Record Mill								Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:		ISM-1892
Mail-states Mail-		Multi factor	Multi-factor authentication is used to authenticate users to their			Multi Footor				
Multi-factor authentication is used to authenticate users to bind-party formation plants and the process, since or communicate their functional intersects With Multi-factor authenticates in used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to authenticate users of data. Mil-factor authentication is used to	ML3-P3			Functional	Intersects With		IAC-06		8	
Multi-factor authentication in such to submit a submit or brind-party authenticates are to third-party authentication in such to authenticate users to third-party authentication submit or authenticate users to detail authentication submit or authenticate users of data. Multi-factor authentication is used to authenticate users of data authenticates in used to authenticate users of data authenticates in used to authenticate users of data. Multi-factor authentication is used to authenticate users of data authenticates in used to authenticate users of data. Multi-factor authentication is used to authenticate users of data authenticates in used to authenticate users of data. Multi-factor authentication is used to authenticate users of data authenticates in used to authenticate users of data. Multi-factor authentication is used to authenticate users of data authenticates in used to authenticate users of data. Multi-factor authentication is used to authenticate users of data authenticates in used to authenticate users of data authentication in used to authenticate users of data authenticates in used to authenticate users of data authenticates in users to authenticate users of data authenticates in users to authenticate users of data authenticates in users to authenticate in users to authenticate in users to authenticate in users to authenticate in u										
Mil-Factor authentication generation's sensitive outnomer data. Mil-Factor authentication is used to authenticate outnomer to online dustromer average and process, store or communicate ensuring engagement of the sensitive outnomer data. Mil-Factor authentication outnomer envices that process, store or communicate ensuring environment of environment environment of environment environmen								Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access;		ISM-1893
Multi-factor authentication is used to authenticate outsomer stock. Multi-factor authentication is used to authenticate outsomer show authentication of the process, store or communicate sensitive outsomer services that process, store or communicate sensitive outsomer services to critical TAS that store, transmit endor process and substantial transmit sensitive regulated accounts. Multi-factor substantial transmit sensitive outsomer services to critical TAS that store, transmit endor process and substantial transmit sensitive regulated accounts. Multi-factor substantial sensitive reg	ML3-P3			Functional	Intersects With		IAC-06		8	
ML3-P3 Multi-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer (ML2-P3) ML3-P3 Multi-factor authentication is used to authenticate privileged users or fact authentication (PFA) ML3-P3 Multi-factor authentication is used to authenticate privileged users or fact authenticate privileged users or fact authentication (PFA) ML3-P3 Multi-factor authentication is used to authenticate privileged users or fact authenticate unprivileged users or fact authenticate users or data appositories. ML3-P3 Multi-factor authentication is used to authenticate users or data appositories. Functional Intersects With Authority (ML3-P3 to the factor authentication used to authenticate users or data appositories. Functional Intersects With Authority (ML3-P3 to the factor authentication used to authenticate users or data appositories. ML3-P3 Multi-factor authentication uses ather: something users have that is unlocked by something users have that is unlo		aumentication	organisation's sensitive customer data.			Authentication (MFA)				
Mild-factor authentication is used to authenticate customers to online customer services that process, store or communicate sensitive customer and/services (fact); and or customer data. ML3-P3 Multi-factor authentication is used to authenticate privileged users of authenticate privileged users of authentication is used to authenticate privileged users of authentication is used to authenticate privileged users of authentication is used to authenticate unprivileged users of data appeals of authentication is used to authenticate unprivileged users of data appeals of authentication is used to authenticate unprivileged users of data appeals of authentication is used to authenticate users of data appeals of authentication is used to authenticate users of data appeals of authentication is used to authenticate users of data appeals of authentication used to authenticate users of data appeals of authentication used to authenticate users of data appeals of authentication used to authenticate users of data appeals of authentication used for authentication users have and something users hav								Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:	-	ISM-1681
ML3-P3 Multi-factor authentication Multi-factor authentication		Multi factor				Multi East		(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or		
ML3-P3 Multi-factor authentication is used to authenticate privileged users of authentication is used to authenticate privileged users of systems. ML3-P3 Multi-factor authentication is used to authenticate unprivileged users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication uses of bare consisting users have that is unlocked by contenting users have that is unlocked by contenting users know or are. ML3-P3 Multi-factor authentication used for authentication used for authentication used of authentication users of online evides is phishing-resistant. ML3-P3 Multi-factor authentication used for authentication used for authentication used of authentication used for authen	ML3-P3			Functional	Intersects With		IAC-06		8	
Multi-factor authentication authentication sused to authenticate unprivileged users of systems. Multi-factor authentication authenticate unprivileged users of systems. Multi-factor authentication for systems. Multi-factor authentication for systems. Multi-factor authentication for systems. Multi-factor authentication is used to authenticate users of data repositories. Multi-factor authentication for systems. Multi-factor authentication uses either systems for systems. Multi-factor authentication for systems. Multi-factor authentication used for authenticating users know or are. Multi-factor authentication used for authentication users for such authentication for systems. Multi-factor authentication used for authentication users for such authentication for systems. Multi-factor authentication used for authentication users for such authentication for systems. Multi-factor authentication users f										
ML3-P3 authentication of systems. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication is used to authenticate users of data repositories. ML3-P3 Multi-factor authentication uses either something users have and something users have that is unlocked by something users have that is unlocked by something users have that is unlocked by something users have or are. ML3-P3 Multi-factor authentication was either enterored. ML3-P3 Multi-factor authentication was either something users have and something users have that is unlocked by something users of online are vices is phishing resistant. ML3-P3 Multi-factor authentication was deformed intersects with authentication (MFA) Multi-factor authentication used for authentication (MFA) for: (1) Remote networks access; (2) Tillid-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data. ML3-P3 Multi-factor authentication used for authentication used for authentication (MFA) for: (1) Remote networks access; (2) Tillid-party Technol	ML3-P3	authentication	systems.	Functional	Intersects With	Privileged Accounts	IAC-06.3	access for privileged accounts.	8	
MI3-P3 Multi-factor authentication is used to authenticate users of data repositories. Multi-factor authentication is used to authenticate users of data repositories. Functional Intersects With Authentication (MFA) MI3-P3 Multi-factor authentication uses either something users have and something users have and something users have that is unlocked by something users have and something users have and something users have that is unlocked by something users have and something users have that is unlocked by something users of online and the intersects with a full-factor authentication used for authenti	ML3-P3			Functional	Intersects With		IAC-06.2	network access for non-privileged accounts.	8	
ML3-P3 Multi-factor authentication Multi-factor authentication Multi-factor authentication ML3-P3 Multi-factor authentication Multi-factor authentication Multi-factor authentication Multi-factor authentication Multi-factor authentication Multi-factor authentication Multi-factor Aut								Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for: (1) Remote network access;	1	ISM-1505
Multi-factor authentication was either something users have and something users know, or are. Multi-factor authentication uses either something users have that is unlocked by something users know or are. Multi-factor authentication uses either something users have that is unlocked by something users know or are. Multi-factor authentication uses either something users have that is unlocked by something users know or are. Multi-factor authentication uses either something users know or are. Multi-factor authentication used for authenticating users of online services is phishing-resistant. Multi-factor authentication used for authenticating users of online services is phishing-resistant. Multi-factor authentication used for authenticating users of online services is phishing-resistant. Multi-factor authentication used for authenticating customers of functional intersects With Authentication (MFA) (MILTi-factor authentication used for authentication (MFA) (MILTi-factor authentication used for authentication used for authentication (MFA) (MILTi-factor authentication used for authentication u	ML3-P3			Functional	Intersects With		IAC-06		8	
Multi-factor authentication was either something users have and something users know, or something users have that is unlocked by something users know or are. Multi-factor authentication uses either something users know or are. Multi-factor authentication (MFA) Multi-factor authentication used for authenticating users of online services is phishing-resistant. Multi-factor authentication was for authentication used for authenticating users of online services is phishing-resistant. Multi-factor authentication was for authentication used for authenticating users of online services is phishing-resistant. Multi-factor authentication was for authentication used for authenticating users of online services is phishing-resistant. Multi-factor authentication was for authentication used for authenticating users of online services is phishing-resistant. Multi-factor authentication was for authentication used for authentication used for authentication was										
ML3-P3 Multi-factor authentication uses either something users have and something users have made and something users have made and something users have that is unlocked by something users have or are. ML3-P3 Multi-factor authentication ML3-P3 Multi-factor authentication Multi-factor authentication Multi-factor authentication Multi-factor authentication Multi-factor authentication used for authenticating users of online services is phishing-resistant. Multi-factor Authentication Multi-factor Automated mechanisms exist to enforce Multi-factor authentication (MFA) for: (1) Remote networis. access; (2) Tild-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process 8 Multi-factor (1) Remote networis. access; (2) Tild-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process 8 Multi-factor (1) Remote networis. access; (2) Tild-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process 8 Multi-factor (1) Remote networis. access; (2) Tild-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process 8 Multi-factor (1) Remote networis. access; (2) Tild-party Technology Assets, Applications and/or Services (TAAS); and/or (3) Non-console access to critical TAAS that store, transmit and/or process 8 Multi-factor (1) Remote networis. access;								Automated mechanisms exist to enforce Multi-Factor Authentication (MFA) for:		ISM-1401
ML3-P3 authentication something users know or are. ML3-P3 Multi-factor authentication used for authenticating users of online services is phishing-resistant. Multi-factor authentication which is phishing-resistant. Multi-factor authentication used for authenticating customers of Functional Intersects With Authentication (MFA) Multi-factor which is phishing-resistant. Multi-factor which is phishing-resistant which is phishing-resistant. Multi-factor which is phishing-resistant which is phishing-resistant. Multi-factor which is phishing-resistant which is phishing-resistan		Multi-factor				Multi-Factor		(2) Third-party Technology Assets, Applications and/or Services (TAAS); and/ or		
ML3-P3 Multi-factor authentication used for authenticating users of online services is phishing-resistant. Multi-factor authentication used for authenticating users of online services is phishing-resistant. Functional Intersects With Authentication (MFA) Multi-factor Services (TAS): and/ or (S) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data. Multi-factor Multi-factor Multi-factor suthentication used for authentication used for authentication (MFA) for: (1) Remote networks access; (2) Tillid-party Technology Assets, Applications and/or Services (TAS): and/ or S) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data. Multi-factor Multi-factor Multi-factor suthentication used for authentication (MFA) for: (1) Remote networks access; (2) Tillid-party Technology Assets, Applications and/or Services (TAS): and/ or S) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data. ML3-P3 Multi-factor Multi-factor Multi-factor suthentication (MFA) for: (1) Remote networks access; (2) Tillid-party Technology Assets, Applications and/or Services (TAS): and/ or S) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data. ML3-P3 Multi-factor Multi-factor suthentication (MFA) for: (1) Remote networks access; (2) Tillid-party Technology Assets, Applications and/or Services (TAS): and/ or S) Non-console access (TAS): and/ or S) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data. ML3-P3 Multi-factor ML3-P3 Multi-factor suthentication (MFA) for: (1) Remote network access; (2) Tillid-party Technology Assets, Applications and/or Services (TAS): and/or S) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data. (3) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data.	ML3-P3			Functional	Intersects With		IAC-06		8	
ML3-P3 Multi-factor authentication used for authenticating users of online services is phishing-resistant. Multi-factor authentication used for authenticating users of online services is phishing-resistant. Functional Intersects With Authentication (MFA) Multi-factor Services (TAS): and/ or (S) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data. Multi-factor Multi-factor Multi-factor suthentication used for authentication used for authentication (MFA) for: (1) Remote networks access; (2) Tillid-party Technology Assets, Applications and/or Services (TAS): and/ or S) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data. Multi-factor Multi-factor Multi-factor suthentication used for authentication (MFA) for: (1) Remote networks access; (2) Tillid-party Technology Assets, Applications and/or Services (TAS): and/ or S) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data. ML3-P3 Multi-factor Multi-factor Multi-factor suthentication (MFA) for: (1) Remote networks access; (2) Tillid-party Technology Assets, Applications and/or Services (TAS): and/ or S) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data. ML3-P3 Multi-factor Multi-factor suthentication (MFA) for: (1) Remote networks access; (2) Tillid-party Technology Assets, Applications and/or Services (TAS): and/ or S) Non-console access (TAS): and/ or S) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data. ML3-P3 Multi-factor ML3-P3 Multi-factor suthentication (MFA) for: (1) Remote network access; (2) Tillid-party Technology Assets, Applications and/or Services (TAS): and/or S) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data. (3) Non-console access to critical TAS that store, transmit and/or process sensitive/regulated data.										
ML3-P3 Putt-factor authentication seed of aut								(1) Remote network access;	1	ISM-1872
ML3-P3 Multi-factor authentication used for authenticating customers of ML3-P3 authentication and or such process of the such authentication and or such process (TAS); and/or (Third-party Technology Assets, Applications and/or Services (TAS); and/or (TAS	ML3-P3			Functional	Intersects With		IAC-06		8	
ML3-P3 Multi-factor Multi-factor authentication used for authenticating customers of Multi-factor Multi-factor authentication used for authenticating customers of Functional Intersects With Authentication (MEA) IAC-06 (3) Non-console access to critical TAAS that store, transmit and/or process 8										
ML3-P3 Multi-factor authentication used for authenticating customers of ML3-P3 authentication used for authenticating customers of Functional Intersects With Authentication (MEA) Intersects With A										ISM-1874
ML3-P3 authorization in authorization in authorization in a second public projected authorization in a second public project of authorization in a second public project pu		Multi-factor	Multi-factor authentication used for authenticating customers of			Multi-Factor		(1) Remote network access; (2) Third-party Technology Assets, Applications and/or Services (TAAS); and/or		
	ML3-P3			Functional	Intersects With		IAC-06	(3) Non-console access to critical TAAS that store, transmit and/or process	8	



Secure Controls Framework (SCF) 6 of 9

			STRM	STRM			Secure Controls Framework (SCF)	Strength of	
FDE#	FDE Name	Focal Document Element (FDE) Description	Rationale	Relationship	SCF Control	SCF#	Control Description	Relationship (optional)	Notes (optional)
ML3-P3	Multi-factor	Multi-factor authentication used for authenticating users of systems is	Functional	Intersects With	Multi-Factor	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	8	ISM-1682
Picara	authentication	phishing-resistant.	runctionat	illeisecis Willi	Authentication (MFA)	IAC-00	(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	8	
	Multi-factor	Multi-factor authentication used for authenticating users of data			Multi-Factor		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		ISM-1894
ML3-P3	authentication	repositories is phishing-resistant.	Functional	Intersects With	Authentication (MFA)	IAC-06	(3) Non-console access to critical TAAS that store, transmit and/or process sensitive/regulated data.	8	
							Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:		ISM-1683
ML3-P3	Multi-factor authentication	Successful and unsuccessful multi-factor authentication events are centrally logged.	Functional	Intersects With	Content of Event Logs	MON-03	(1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred;	5	
	dationiodion	contany to a con-					(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.		
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 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-P3	Multi-factor authentication	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-P3	Multi-factor authentication	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-P3	Multi-factor authentication	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-P3	Multi-factor	Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur	Functional	Intersects With	Event Log Analysis &	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	authentication	or are discovered.	runctionat	intersects with	Triage	MON-17	Mechanisms exist to timely-report incidents to applicable:	5	ISM-0140
ML3-P3	Multi-factor authentication	Cybersecurity incidents are reported to ASD as soon as possible after they occur or are discovered.	Functional	Subset Of	Incident Stakeholder Reporting	IRO-10	(1) Internal stakeholders; (2) Affected clients & third-parties; and (3) Regulatory authorities.	10	
							Mechanisms exist to cover: (1) Preparation:		ISM-1819
ML3-P3	Multi-factor	Following the identification of a cybersecurity incident, the	Functional	Subset Of	Incident Handling	IRO-02	(2) Automated event detection or manual incident report intake; (3) Analysis;	10	
ML3-P3	authentication	cybersecurity incident response plan is enacted.	runctionat	Subset Of	incident Handling	INO-02	(s) Analysis; (4) Containment; (5) Eradication: and	10	
	Restrict administrative	Requests for privileged access to systems, applications and data			Privileged Account		(6) Recovery Mechanisms exist to restrict and control privileged access rights for users and		ISM-1507
ML3-P4	privileges Restrict administrative	repositories are validated when first requested. Requests for privileged access to systems, applications and data	Functional	Intersects With	Management (PAM) Management Approval	IAC-16	Technology Assets, Applications and/or Services (TAAS). Mechanisms exist to restrict the assignment of privileged accounts to	5	ISM-1507
ML3-P4	privileges Restrict administrative	repositories are validated when first requested. Privileged access to systems, applications and data repositories is	Functional	Intersects With	For Privileged Accounts Privileged Account	IAC-21.3	management-approved personnel and/or roles. Mechanisms exist to restrict and control privileged access rights for users and	5	ISM-1647
ML3-P4	privileges Restrict administrative	disabled after 12 months unless revalidated. Privileged access to systems and applications is disabled after 45 days	Functional	Intersects With	Management (PAM) Disable Inactive	IAC-16	Technology Assets, Applications and/or Services (TAAS). Automated mechanisms exist to disable inactive accounts after an organization-	3	ISM-1648
ML3-P4	privileges	of inactivity.	Functional	Intersects With	Accounts Dedicated Privileged	IAC-15.3	defined time period.	8	ISM-0445
ML3-P4	privileges	Privileged users are assigned a dedicated privileged user account to be used solely for duties requiring privileged access.	Functional	Equal	Account	IAC-16.4	Mechanisms exist to assign dedicated privileged user accounts to be used solely for duties requiring privileged access.	10	
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	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	5	ISM-1508
	Restrict administrative	their duties. Privileged user accounts (excluding those explicitly authorised to			Non-Privileged Access for		organizational business functions. Mechanisms exist to prohibit privileged users from using privileged accounts,		ISM-1175
ML3-P4	privileges	access online services) are prevented from accessing the internet, email and web services. Privileged user accounts explicitly authorised to access online services	Functional	Intersects With	Non-Security Functions	IAC-21.2	while performing non-security functions. Mechanisms exist to utilize the concept of least privilege, allowing only authorized	5	ISM-1883
ML3-P4	Restrict administrative privileges	are strictly limited to only what is required for users and services to undertake their duties.	Functional	Subset Of	Least Privilege	IAC-21	access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	10	1317-1003
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 to a dedicated machine.	10	ISM-1898
ML3-P4	Restrict administrative	Privileged users use separate privileged and unprivileged operating	Functional	Intersects With	Privileged Account	IAC-16	Mechanisms exist to restrict and control privileged access rights for users and	5	ISM-1380
ML3-P4		environments. Privileged operating environments are not virtualised within	Functional	Subset Of	Management (PAM) Privileged Environments	SEA-22	Technology Assets, Applications and/or Services (TAAS). Mechanisms exist to prevent privileged operating environments from existing within unprivileged operating environments. including physical or virtual	10	ISM-1687
ML3-P4	privileges Restrict administrative	unprivileged operating environments. Unprivileged user accounts cannot logon to privileged operating	Functional	Subset Of	Role-Based Access	IAC-08	deployments of Technology Assets, Applications and/or Services (TAAS). Mechanisms exist to enforce Role-Based Access Control (RBAC) for Technology Assets, Applications, Services and/or Data (TAASD) to restrict access to	10	ISM-1688
	privileges Restrict administrative	environments. Privileged user accounts (excluding local administrator accounts)			Control (RBAC) Non-Privileged Access for		individuals assigned specific roles with legitimate business needs. Mechanisms exist to prohibit privileged users from using privileged accounts,		ISM-1689
ML3-P4	priviteges	cannot logon to unprivileged operating environments. Just-in-time administration is used for administering systems and	Functional	Intersects With	Non-Security Functions Privileged Account	IAC-21.2	while performing non-security functions. Mechanisms exist to restrict and control privileged access rights for users and	5	ISM-1649
ML3-P4	privileges Restrict administrative	applications.	Functional	Intersects With	Management (PAM)	IAC-16	Technology Assets, Applications and/or Services (TAAS). Mechanisms exist to conduct remote system administrative functions via a "jump	8	ISM-1387
ML3-P4	privileges	Administrative activities are conducted through jump servers. Credentials for break glass accounts, local administrator accounts	Functional	Subset Of	Jump Server	AST-27	box" or "jump server" that is located in a separate network zone to user workstations. Mechanisms exist to establish and control "emergency access only" accounts.	10	ISM-1685
ML3-P4	privileges	and service accounts are long, unique, unpredictable and managed.	Functional	Intersects With	Emergency Accounts	IAC-15.9	Mechanisms exist to develop, document and maintain secure baseline	8	ISM-1896
ML3-P4	Restrict administrative privileges	Memory integrity functionality is enabled.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	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	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	
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		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
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		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		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		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		Cybersecurity events. 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	5	ISM-1228
ML3-P4	Restrict administrative	Cybersecurity incidents. Cybersecurity incidents are reported to the chief information security officer, or one of their delegates, as soon as possible after they occur	Functional	Intersects With	Event Log Analysis & Triage	MON-17	records from multiple sources. 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		or are discovered. Cybersecurity incidents are reported to ASD as soon as possible after	Functional	Subset Of	Incident Stakeholder	IRO-10	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders;	10	ISM-0140
	privileges	they occur or are discovered.			Reporting		(2) Affected clients & third-parties; and (3) Regulatory authorities. Mechanisms exist to cover:	1	ISM-1819
	Destries .						(1) Preparation; (2) Automated event detection or manual incident report intake;		
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	(3) Analysis; (4) Containment;	10	
							(5) Eradication; and (6) Recovery.		
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



cure Controls Framework (SCF)

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 (optional)
ML3-P5	Application control	Application control is applied to user profiles and temporary folders	Functional	Intersects With	Explicitly Allow / Deny	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist /	(optional) 5	ISM-1870
		used by operating systems, web browsers and email clients. Application control is applied to all locations other than user profiles			Applications Explicitly Allow / Deny		blacklist) applications that are authorized to execute on systems. Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist /		ISM-1871
ML3-P5	Application control	and temporary folders used by operating systems, web browsers and email clients.	Functional	Intersects With	Applications	CFG-03.3	blacklist) applications that are authorized to execute on systems.	5	
ML3-P5	Application control	Application control restricts the execution of executables, software libraries, scripts, installers, compiled HTML, HTML applications and	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	control panel applets to an organisation-approved set. 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
ML3-P5	Application control	Microsoft's recommended application blocklist is implemented.	Functional	Intersects With	Secure Baseline	CFG-02	Mechanisms wist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1544
					Configurations Secure Baseline		consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	_	ISM-1659
ML3-P5	Application control	Microsoft's vulnerable driver blocklist is implemented.	Functional	Intersects With	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
ML3-P5	Application control	Application control rulesets are validated on an annual or more	Functional	Intersects With	Reviews & Updates	CFG-02.1	Mechanisms exist to review and update baseline configurations: (1) At least annually;	8	ISM-1582
	.,,,	frequent basis.					(2) When required due to so; or (3) As part of system component installations and upgrades.	_	
							Mechanisms exist to configure Technology Assets, Applications and/or Services (TAAS) to produce event logs that contain sufficient information to, at a minimum:		ISM-1660
ML3-P5	Application control	Allowed and blocked application control events are centrally logged.	Functional	Subset Of	Content of Event Logs	MON-03	(1) Establish what type of event occurred; (2) When (date and time) the event occurred; (3) Where the event occurred;	10	
PILSTO	Application control	Attowed and brocked application control events are centrary logged.	rancuonat	Subset Of	Content of Event Logs	11014-03	(3) Where the event occurred; (4) The source of the event; (5) The outcome (success or failure) of the event; and	10	
							(6) The identity of any user/subject associated with the event.		
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 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 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-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. Cybersecurity incidents are reported to the chief information security	Functional	Intersects With	Central Review & Analysis	MON-02.2	Automated mechanisms exist to centrally collect, review and analyze audit records from multiple sources. Mechanisms exist to ensure event log reviews include analysis and triage practice	5	ISM-1228 ISM-0123
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 tog reviews include analysis and triage practice that integrate with the organization's established incident response processes.	5	
	Applie 1	Cybersecurity incidents are reported to ASD as soon as possible after	F	0.1	Incident Stakeholder	Inc. :	Mechanisms exist to timely-report incidents to applicable: (1) Internal stakeholders;		ISM-0140
ML3-P5	Application control	they occur or are discovered.	Functional	Subset Of	Reporting	IRO-10	(2) Affected clients & third-parties; and (3) Regulatory authorities.	10	
							Mechanisms exist to cover: (1) Preparation;		ISM-1819
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	(2) Automated event detection or manual incident report intake; (3) Analysis;	10	
		cybersecurity incluent response plan is enacted.					(4) Containment; (5) Eradication; and		
	Restrict Microsoft	Microsoft Office macros are disabled for users that do not have a			Secure Baseline		(6) Recovery. Mechanisms exist to develop, document and maintain secure baseline		ISM-1671
ML3-P6	Office macros	demonstrated business requirement.	Functional	Intersects With	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
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	5	ISM-1674
ML3-P6	Restrict Microsoft	Microsoft Office macros are checked to ensure they are free of malicious code before being digitally signed or placed within Trusted	Functional	Intersects With	Secure Baseline	CFG-02	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1890
	Office macros	Locations. Only privileged users responsible for checking that Microsoft Office			Configurations		consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline		ISM-1487
ML3-P6	Restrict Microsoft Office macros	macros are free of malicious code can write to and modify content within Trusted Locations.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
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	5	ISM-1675
ML3-P6	Restrict Microsoft	Microsoft Office macros digitally signed by signatures other than V3	Functional	Intersects With	Secure Baseline	CFG-02	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	5	ISM-1891
ML3-P6	Office macros	signatures cannot be enabled via the Message Bar or Backstage View.	runctionat	intersects with	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. Mechanisms exist to review and update baseline configurations:	•	ISM-1676
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	(1) At least annually; (2) When required due to so; or	5	
	Restrict Microsoft				Secure Baseline		(3) As part of system component installations and upgrades. Mechanisms exist to develop, document and maintain secure baseline		ISM-1488
ML3-P6	Office macros	Microsoft Office macros in files originating from the internet are blocked.	Functional	Intersects With	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
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	5	ISM-1672
ML3-P6	Restrict Microsoft	Microsoft Office macros are blocked from making Win32 API calls.	Functional	Intersects With	Secure Baseline	CFG-02	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	5	ISM-1673
PILSTO	Office macros	Prictosoft Office fractos are blocked from making winsz API caus.	rancuonat	III (el sects with	Configurations	C1-0-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	,	ISM-1489
ML3-P6	Restrict Microsoft Office macros	Microsoft Office macro security settings cannot be changed by users.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	13111133
ML3-P7	User application	Internet Explorer 11 is disabled or removed.	Functional	Intersects With	Secure Baseline	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1654
	hardening User application				Configurations Secure Baseline		consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	_	ISM-1486
ML3-P7	hardening	Web browsers do not process Java from the internet.	Functional	Intersects With	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	IOM AND
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 occupied system hardening standards	5	ISM-1485
ML3-P7	User application	Web browsers are hardened using ASD and vendor hardening guidance, with the most restrictive guidance taking precedence when	Functional	Intersects With	Secure Baseline	CFG-02	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1412
	hardening	conflicts occur.			Configurations Secure Recoline		consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline		ISM-1585
ML3-P7	User application hardening	Web browser security settings cannot be changed by users.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
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	5	ISM-1667
MI 0 PT	User application	Microsoft Office in blooked from a state of the state of	Europia :	Inter	Secure Baseline	050	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	5	ISM-1668
ML3-P7	hardening	Microsoft Office is blocked from creating executable content.	Functional	Intersects With	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	ь	ISM-1669
ML3-P7	User application hardening	Microsoft Office is blocked from injecting code into other processes.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	rectionisms exist to develop, occurrent and maintain secure basedine configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
ML3-P7	User application	Microsoft Office is configured to prevent activation of Object Linking	Functional	Intersects With	Secure Baseline	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1542
	hardening User application	and Embedding packages. Office productivity suites are hardened using ASD and vendor			Configurations Secure Baseline		consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline		ISM-1859
ML3-P7	hardening	hardening guidance, with the most restrictive guidance taking precedence when conflicts occur.	Functional	Intersects With	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	
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	5	ISM-1823
ML3-P7	User application	PDE software is blocked from croating shill a	Functional	Intersects With	Secure Baseline	CFG-02	consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline applications for Technique (Application and Institute and Institute and Institute and Ins	5	ISM-1670
mL3-P/	hardening	PDF software is blocked from creating child processes. PDF software is hardened using ASD and vendor hardening guidance,	runctional	intersects with	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	ь	ISM-1860
ML3-P7	User application hardening	with the most restrictive guidance taking precedence when conflicts occur.	Functional	Intersects With	Secure Baseline Configurations	CFG-02	rectionisms 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	
ML3-P7	User application hardening	PDF software security settings cannot be changed by users.	Functional	Intersects With	Secure Baseline	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for Technology Assets, Applications and/or Services (TAAS) that are	5	ISM-1824
	nardening User application				Configurations Secure Baseline		consistent with industry-accepted system hardening standards. Mechanisms exist to develop, document and maintain secure baseline	_	ISM-1655
ML3-P7	hardening	.NET Framework 3.5 (includes .NET 2.0 and 3.0) is disabled or removed.	Functional	Intersects With	Configurations	CFG-02	configurations for Technology Assets, Applications and/or Services (TAAS) that are consistent with industry-accepted system hardening standards.	5	IOM ACCA
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 constraint and the producing strandards.	5	ISM-1621
I	1		1	1	1		consistent with industry-accepted system hardening standards.	1	



FDE#	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF#	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
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 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 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-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) Endication; 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 (RTOs) and Recovery Point Objectives (RPOs).	5	ISM-1511
ML3-P8	Regular backups	Backups of data, applications and settings are synchronised 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
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 business 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



Secure Controls Framework (SCF) 9 of 9